

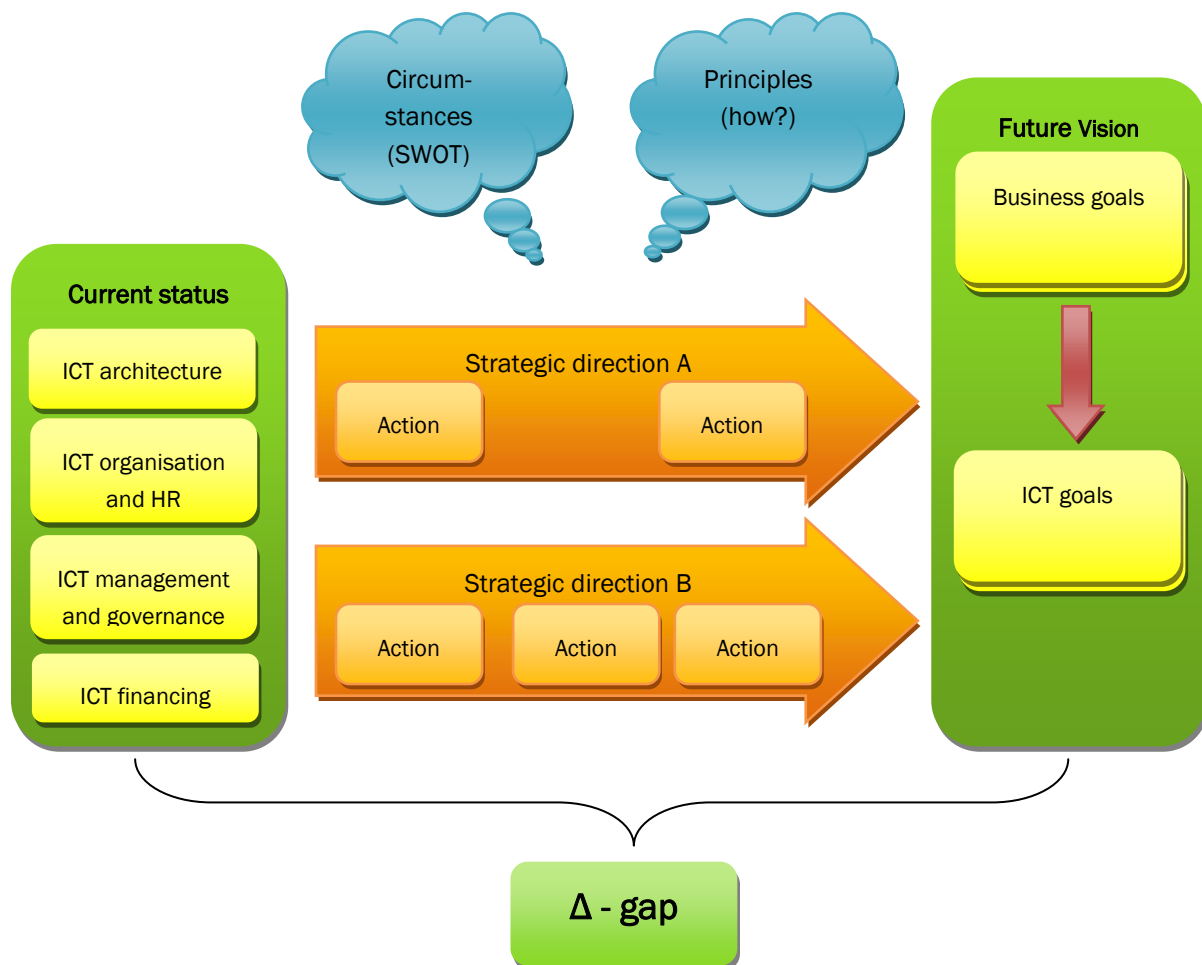
ANNEX

A. METHODOLOGY

This section describes the general approach followed during preparation of the Final ICT Strategy Report. It contains the basic terminology used together with the description of the activities leading to the Report.

A.1. FUNDAMENTAL TERMINOLOGY

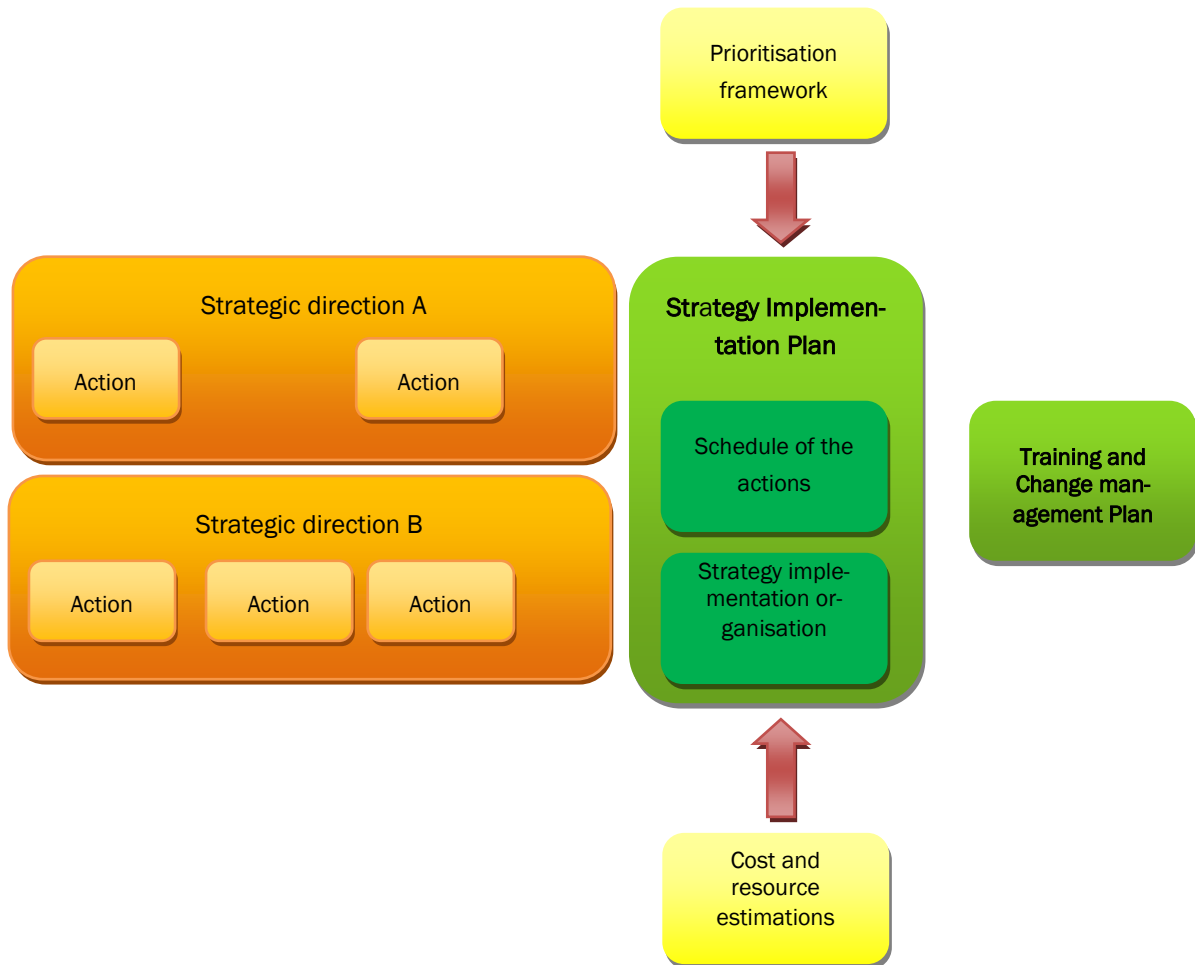
This section describes the terminology used in the ICT Strategy Report. The following diagram gives an overview of the notions and their relationships:



Summarised in one paragraph:

The Consultant's recommended **Future ICT Vision** of the Serbian Justice Sector consists of **ICT goals** which are derived from the **business goals**. To reach these goals the **gap** between the current and future states should be bridged by executing **actions** linked to various large scale **strategic directions** under the conditions determined by **circumstances** detailed in a **SWOT analysis** and overall **principles**.

The ICT Strategy Report is basically an extension of the Penultimate Report by detailed description of the Strategic actions and by cost and resource estimations which lead to a detailed implementation plan. The following diagram gives an overview of notions and terminology:



Summarised in one paragraph:

The Consultant's recommended **Strategy Implementation Plan** of the Justice Sector is the set of all defined **actions** arranged in time using the priorities of the **Prioritization framework** and **Cost and resource estimates**. It also contains the **organisational framework for implementation** and is accompanied by a **Training and Change Management plan** to help smooth and successful implementation

The definition and explanation for the terminology is explained in the following table:

Notion	Definition	Typical question	Example
Current status (Diagnosis)	A descriptive analysis of the current situation of architecture, human resources, ICT management and financing		Workstations are heterogeneous in terms of age, operating systems and office applications
Business goals	Major characteristic of the future state of Justice Sector	What the justice system should look like?	Efficiency
High level ICT goals	Major objectives of the future state of justice ICT services	What are the major focal points of improving the judicial ICT?	Enhance information security
Mid level ICT goals	Detailed characteristics of the future state of Judiciary ICT	By which goals could the ICT contribute to the judicial business objectives?	Performance of end user environment is supporting everyday tasks

Notion	Definition	Typical question	Example
SWOT	Current internal strengths and weaknesses; external opportunities and threats towards judicial ICT	What are the internal and external factors which support or inhibit the changes within judicial ICT?	S: Partly modernised end-user working environment W: ICT equipment partly outdated O: Government level agreement with Microsoft to supply software T: Growing budgetary pressure and expenditure cuts
Gap	The difference between the current state and the desired end state of the strategic time horizon	What is missing from the current state of ICT which is aimed at the desired vision?	5000 current end-user workstations will not satisfy business needs by 2017
Principle	General rules and guidelines about the way the Justice Sector sets about to fulfil its IT mission	What are the considerations and rules when defining and executing strategic actions?	Avoidance of vendor lock-in
Actions	A definite set of activities to achieve a definite result	What to do to achieve the ICT objectives?	“Renew end-user environment with equipment of homogenous software environment and enough power “
Prioritisation Framework	A method to assign priorities to the individual Actions in order to help decision on their implementation.	Which Actions are really important for the Justice sector with their results validating the expected efforts?	Action X is a “Low hanging fruit” meaning that it has a large yield with relatively low investment.

A.2. METHODOLOGY FOR SETTING STRATEGIC GOALS

The strategic goals of the ICT Strategy for the Justice sector are determined using the Balanced Scorecard (BSC) approach. Balanced Scorecard is a strategic performance measurement tool invented by Art Schneiderman, Robert S. Kaplan and David P. Norton at the beginning of the 90's. Its major concept is that the performance of an organisation cannot be simply measured only by financial measures, but consideration of other characteristics of the organisation is essential to ensure a healthy organisation in the long run. The four perspectives of the organisation were defined as:

- *Financial* – measuring the financial performance of the organisation (i.e. profitability, revenue, utilisation of resources, stock levels etc.)
- *Customer (or service)* – measuring the services/products and the aspects important to the customers (i.e. product/service quality, functionality, price, accessibility, brand)
- *Internal business processes (or operational)* – measuring the effectiveness and efficiency of the procedures to satisfy the customers (i.e. cycle times, quality assurance effectiveness, resource needs, etc.)
- *Learning and growth* – measuring factors contributing to the long term success of the organisation (employee skills, IT support of processes, internal culture)

According to the original concept of Balanced Scorecard, it was a measurement, reporting and management tool, but later it was widened to other areas of strategic management. One of the first improvements was to use BSC as a strategy definition tool helping the organisation to set clear, measurable goals and reveal their interrelations. Other extension was the consideration of public institutions for which the financial measurement is preceded by the need to satisfy their stakeholders' expectations. These expectations may be formulated as the real objectives of the organisation. These might include for example compliance with the regulations or generating value for the society.

During the Workshops with the representatives of the Ministry and from judicial institutions, some general ICT goals were determined and later refined to 44 mid-level ICT goals. Another input to determine the ICT

goals were provided by the analysis and the problems contained in the Diagnostic Report and the interviews with the appointed institutions.

The mid-level ICT goals were validated by determining their contribution to the five pillars of the Justice Reform Strategy:

- Independence
- Impartiality and Quality of Justice
- Competence
- Accountability
- Efficiency of the Judiciary and backlog reduction

We regarded an ICT goal strategic only if a significant contribution could be measured to the above pillars. Finally the ICT goals were grouped into 18 groups to provide a manageable set of strategic directions. The same ICT goal could be assigned to more than one group.

A.3. METHODOLOGY FOR SWOT ANALYSIS AND GAP ANALYSIS

SWOT analysis

SWOT analysis is a powerful tool in Strategy development to assist in determination of the actions leading to a desired goal. The analysis leans on the following factors:

- Internal factors
 - **Strengths** – the existing helpful attributes of the Justice Sector which are a good base for achieving the goals
 - **Weaknesses** – the existing harmful attributes of the Justice Sector which form an obstacle to achieve the goals
- External factors (the Justice Sector has no direct effect on these factors)
 - **Opportunities** – the existing or anticipated environmental attributes of the Justice Sector which may help the achievement of the goals
 - **Threats** – the existing or anticipated environmental attributes of the Justice Sector which may endanger the achievement of the goals

Internal factors were derived from the Diagnostic Report by evaluating the facts. They are structured according to Report structure as follows:

- ICT architectural factors
- ICT staff, human capital factors
- ICT operational factors
- ICT financial factors

External factors were determined from information gathered during interviews about the external environment of the Justice Sector and from general ICT trends.

Gap analysis

Gap analysis compares the current status with the desired strategic goals and the difference between the current and desired situation are to be bridged by the strategic actions. Whenever quantifiable, gap analysis measures the distance between current and desired states.

Consequently the basic “units” of gap analysis are the ICT goals and whenever applicable, the gap is described in terms of architecture, human resources, organisation and operational viewpoints.

A.4. METHODOLOGY FOR DETAILED ACTION PLANNING

Consultant's recommended Strategic actions constitute the essence of the ICT Strategy, since they describe what to do in order to achieve the recommended ICT goals.

Action planning was done in two phases:

- At first the desired future vision description was prepared for each strategic direction. This detailed description summarizes the relevant part of the ICT goals, the SWOT analysis and provides solutions for closing the gap between the current and desired states.
- Next follows a brief description of the specific actions to be executed.

During detailed action planning the prerequisites for the various recommended Strategic actions were determined. These prerequisites mostly include other Strategic actions but some other preconditions were also described if needed.

For each recommended Strategic action the major steps of carrying out the action were defined together with a cost and resource estimation of the Consultant. As it is described in Detailed Implementation Plan Section , the cost and resource estimates were made on a high level assigning cost and resource bands for each action. These cost and resource bands allow the overall prioritisation of the Strategic actions but detailed resource planning should be done during the preparatory phases of each implementation projects. For each action also the estimated timeframe was given in quarters of years units.

Finally the major risks of the Strategic action implementations were determined, assessed and mitigation for them was provided.

A.5. METHODOLOGY FOR IMPLEMENTATION ROADMAP DEFINITION

The Implementation roadmap is the assembly of all the recommended Strategic actions for a single possible schedule for the next 5 years. During scheduling the following principles were considered:

- Prerequisites of a Strategic action has to precede the action itself
- Strategy execution should be evenly distributed in the available timeframe
- First years of Strategy Implementation should require less financial resources in order to be able to acquire, define donor funds for larger projects

The Implementation Roadmap contains all recommended Strategic actions, but their execution depends on the availability of financial and human resources. This roadmap needs finalisation whenever the to-be-executed Strategic actions are selected from the full set of Strategic actions.

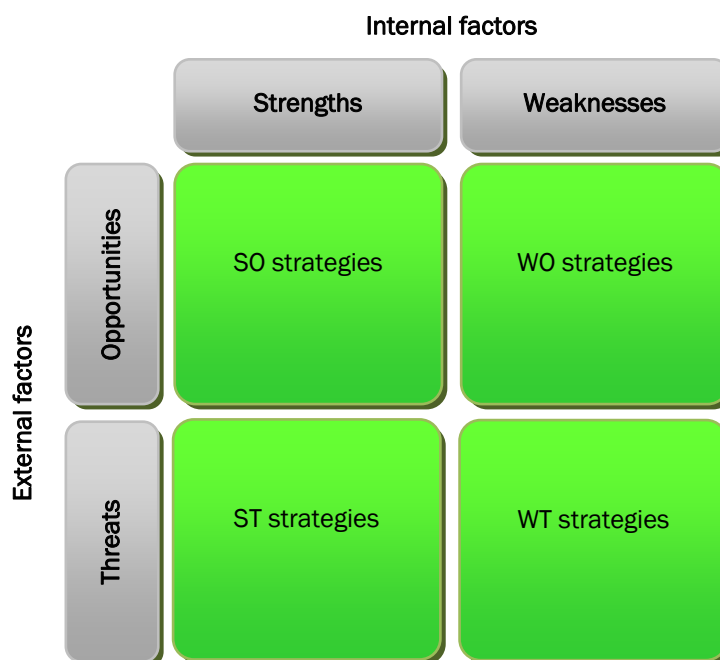
B. SWOT ANALYSIS

This section contains an overall SWOT analysis regarding the ICT sector with some institutional aspects as well. The Internal factors of the SWOT analysis are grouped into the same major domains as the Diagnostic Report was built up, namely ICT architecture, ICT human capital, ICT operations and ICT financials.

B.1. USING SWOT ANALYSIS TO IDENTIFY TARGETS AND STRATEGIES

The SWOT analysis does not stand in itself, but it is used to identify take-off points from the current situation. In a simple approach Strength are the factors to build future plans, Weaknesses are to be overcome by actions, Opportunities present options for change and Threats are factors to avoid or reduce in the future by actions.

Using a more complex approach, the SWOT factors are arranged into a matrix:



The four quadrants of the SWOT matrix is analysed to define development actions, as follows:

SWOT Quadrant I - Strengths/Opportunities (SO)

This quadrant focuses on goals and strategies that take advantage of Ministry's core strengths to pursue the best opportunities at its disposal. This is particularly important if the opportunities are short-lived. An example would be to use the experience of the State-of-the art Case Management Systems implemented recently (*a Strength*), exploit available donor funds (*an Opportunity*) to roll-out the systems for a wider circle of institutions.

SWOT Quadrant II - Strengths/Threats (ST)

This quadrant focuses on goals and strategies that utilize Ministry's strengths to actively eliminate or reduce threats you are facing. An example would be to utilize the well established organisational responsibilities to finance and manage donor projects (*a Strength*) to handle risks of growing maintenance costs (*a Threat*) by

implementing a Total Cost of Ownership calculation model to reveal expected operation costs and be prepared for them.

SWOT Quadrant III-Weaknesses/Opportunities (WO)

This quadrant focuses on goals and strategies that can help the Ministry to open up opportunities down the road by working to reduce some of the existing weaknesses. Actions of this quadrant may help to execute long-term improvements. An example would be to rely on the governmental contract with Microsoft (*an Opportunity*) to homogenise the currently partly outdated ICT equipment (*a Weakness*).

SWOT Quadrant IV - Weaknesses/Threats (WT)

Finally, this quadrant focuses on goals and strategies that can help the Ministry to mitigate and avoid threats that could result from the weaknesses. You could do this by eliminating the weaknesses and turning them into strengths, or by developing defensive strategies to reduce the likelihood or severity of the threat.

An example would be to overcome the risk of drawing away talented ICT professionals and well-trained experts to the private sector (*a Threat*) because of lack of developed career paths for ICT employees (*a Weakness*) by implement conscious human resource management procedures within IT unit focusing on trainings, motivation and promotion opportunities.

Naturally not all possible combination of factors along the above described lines will produce a meaningful strategic direction. The SWOT analysis provides a good initial standing point for the analysis, but other factors, like goals derived from business strategy should also be considered.

B.2. FACTORS OF THE SWOT ANALYSIS

In case of internal factors, the Strengths and Weaknesses are grouped along the major domains of the ICT Strategy

Strengths

ICT architecture:

- Well developed network infrastructure (WAN and local) at most sites
- Recent efforts to modernize key data centres
- Partly modernized end-user working environment
- State of the art Case Management systems at some institutions
- New Case Management systems are developed on same platform
- Basic security measures have been taken (anti-virus, spam filtering)
- Several mid-range servers will be available for other duties after SAPS implementation

ICT staff human capital:

- Loyal IT staff, popularity of public administration jobs leads to longer-term employment of judiciary IT staff
- Experience of ICT staff in operation of justice systems
- Enthusiastic and competent training and IT staff

- Implementation Plan of the System for Monitoring and Evaluation exists
- Judicial Academy has a vision on deeper involvement in IT related trainings
 - Well-equipped training facilities in four different regions

ICT operations:

- Existing coordination of ICT development efforts
- Well established organisational responsibilities to finance and manage donor projects

Weaknesses

ICT architecture:

- No practice of the use of electronic signatures
- Insufficient or inefficient peripherals (scanning capacity, desktop printers)
- Electronic archiving is not implemented
- Document exchange with counterparts is paper based
- Fragmented case management systems, 3 separate ongoing implementations (SAPS, SAPO, SAPA)
- No information sharing standards defined on the semantic level
- No other communication channels except for web portal exist or planned
- Statistical ICT system capabilities are underdeveloped
- Insufficient security measures (logging) and awareness, attitude and knowledge about data security issues
- Inconsistent progress in implementing ICT (courts and prosecution offices)
- No separate ICT infrastructure and ICT staff for prosecution offices
- ICT equipment partly outdated and should be replaced until the rollout of current case management developments
- Communication bandwidth is not wide enough at certain locations

ICT staff human capital:

- ICT staff numbers too low, no specialization of ICT roles
- Limited number of trainings and other development opportunities
- No special selection and testing of ICT staff in the hiring process
- In some Justice Sector institutions, salaries of ICT professionals are lower compared to other Justice Sector employees and the private sector
- Judicial Academy lacks the full ICT support for the whole training cycle
- No developed career path for ICT employees
- Non-ICT staff ICT skills are heterogeneous
- End user affinity to usage of ICT tools is varying from low to high

ICT operations:

- IT operations are fragmented (staff, procurement, maintenance)
- Lack of "user participation" in development projects
- No means to enforce the ICT regulations issued by the Ministry of Justice and Public Administration
- Lack of established performance measurement system for ICT
- Lack of formalised methods/forums to involve HJC and SPC in ICT related decisions

ICT Financials:

- Ministry budget is heavily constrained
- Budget planning is constrained by governmental accounting rules, the budget structure is not reflecting all aspects of ICT costs

Opportunities

- Possible synergies from the new ministry structure - Public Administration added to MoJ
- EU accession process opens new funds for developments
- Continuing availability of donor funding to finance developments
- Price of new technologies and unit price of some capacities (i.e. storage) are decreasing,
- ICT Strategy is under preparation to give a framework to and coordinate development efforts
- Governmental e-Government development efforts may provide additional resources
- Increased requests for e-Services from the public, from legal entities, from attorneys, from public notaries and private enforcers
- New legal regulations affecting electronic state administrations (i.e. planned law on data security)
- Governmental contract with Microsoft to cover licences for Office products
- Create institutional identity through unified vision of all judicial bodies
- Availability of international standards for regulation of various aspects of ICT developments and operations
- Knowledgeable business partners having accumulated deep knowledge of the justice ICT
- Access to qualified ICT staff on the local IT market
- Continuing cooperation with the NGO's and businesses, aiming to organise common training events
- New trends in trainings: classroom and computer training, coaching and mentoring at the workplace, self-study

Threats

- Perpetual changes in the institutional framework of the Justice Sector
- Growing maintenance costs as a result of donor-funded ICT developments and purchases
- Growing budgetary pressure and expenditure cuts
- Talented ICT professionals, well-trained experts / trainers may be drawn away to the private sector with a promise of better salaries and career paths
- Reluctance of other governmental agencies to establish electronic data channels
- Lower level regulatory items are missing (i.e. bylaws for Digital Signature) or are created very slowly

C. STRATEGIC GOALS

This Section contains the lower level ICT goals to be aimed at within the strategic time horizon. The goals together with the SWOT analysis would provide the basis of detailed planning of recommended Strategic actions.

Within a strategic time horizon, the Justice Sector organisations may formulate several objectives at varying levels. Some objectives may be regarded as “strategic”, some others have only local effects and are only “tactical”. In this section a unified view is provided on the strategic level ICT goals. The ICT goals are linked to the long term business goals (the 5 pillars) of the Justice Reform Strategy to demonstrate coherence and alignment of ICT with the business expectations.

In Judiciary ICT Strategy the Balanced Scorecard approach is used to formulate the strategic goals of the sector. The perspectives used are the following:

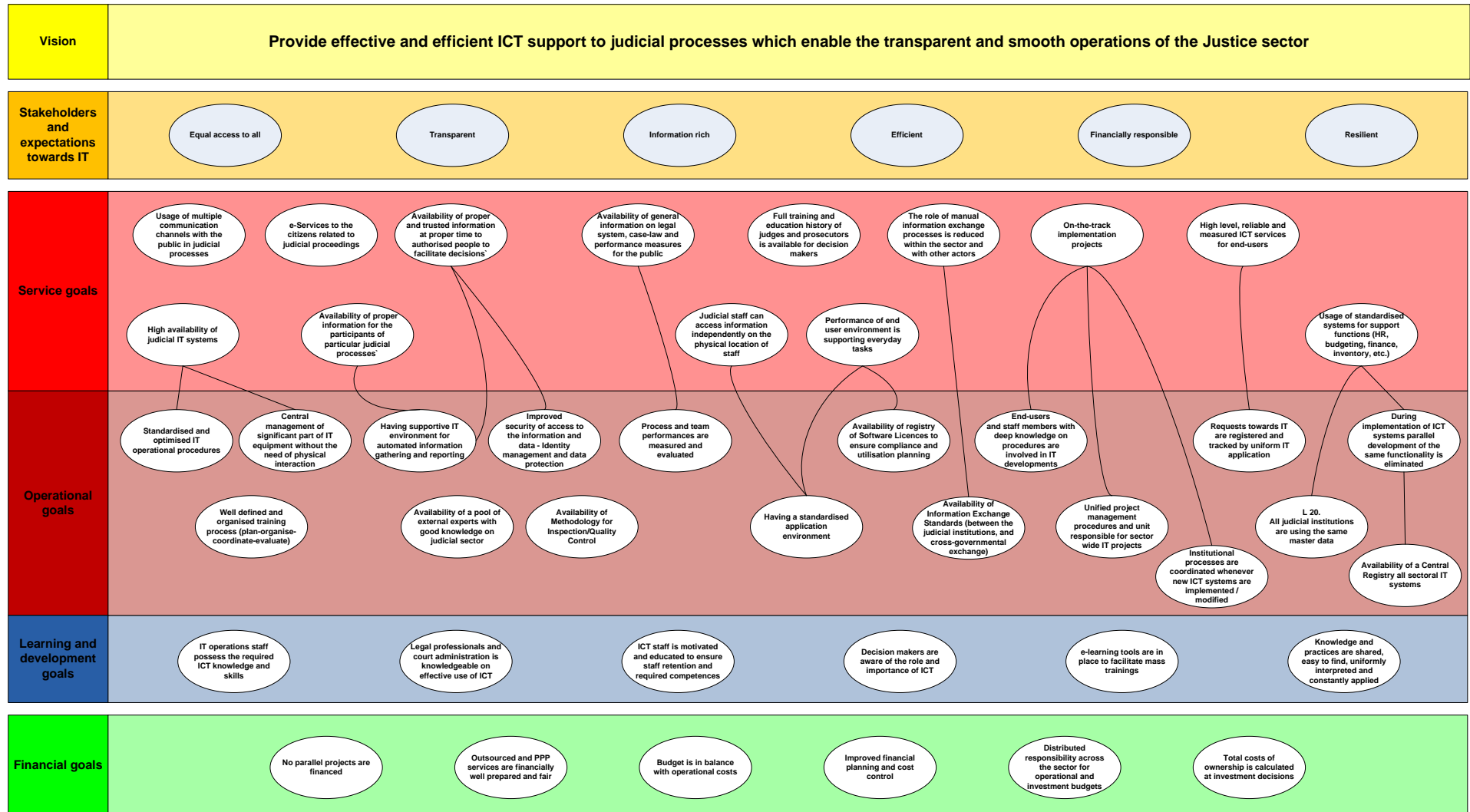
- Service goals
- Operational goals
- Learning and development goals
- Financial goals

Above all goals there are the expectations of stakeholders. From strategic perspective stakeholders are the following:

- natural and legal persons taking part in any judicial procedure
- staff of the sector using ICT tools for their tasks
- justice professionals having role in the procedures (i.e. advocates/lawyers)
- Government of Serbia and other governmental institutions participating in judicial procedures
- European Union

According to the used approach, several goals are formulated for each of the above four perspectives. The goals are described as a desired state and no exact measures are attached to them, since setting a fully accepted measure set together with the exact calculation methods and desired values is a lengthy effort – partly undertaken during strategy finalisation – and would require the formulation of measurable goals in the Justice System Reform Strategy.

The goals are presented on the following diagram, where each oval represents a goal, and whenever there is a tighter cause-effect relationship between two goals then this fact is indicated by a link between them.



D. RECOMMENDED ICT VISION

This section contains the Consultant's recommendation on the overall future vision of ICT from architectural, organisational and governance viewpoints.

D.1. ARCHITECTURAL VISION

Over the next five years, the Ministry of Justice and Public Administration should establish sustainable and reliable ICT infrastructure, to ensure that all justice sector systems are available to end users, regardless of their location.

Basically there are two alternative visions for the infrastructure, a centralised one and a distributed one.

The characteristics of the centralised infrastructure are:

1. Data-centres and networking hubs in Belgrade, Novi Sad, Kragujevac and Niš, implementing high-availability and fail-over mechanisms for both hardware and network. As an alternative - if the e-Government infrastructure of the Serbian Government will have the sufficient capacities - a governmental cloud may be viable option compared to the 4 judicial data centres.
2. Wide Area Network, providing sufficient bandwidth and reliability to support centralized, service-oriented software architecture.
3. Enterprise Service Bus or similar middleware that facilitates interoperability and information exchange between internal and external systems.

The Ministry of Justice and Public Administration has already taken important steps in this direction, with the establishment of data-centres in Belgrade and its strategic orientation towards centralized, Service Oriented Architecture during the development of the latest case management systems.

Because of scarce financial resources, the MoJPA will need additional, donor funds, to renew and upgrade the ICT infrastructure to the optimal level. However, even with additional funding, compromises will have to be made for best allocation of available resources to those aspects of the ICT infrastructure that would provide the largest benefits to the entire sector.

The characteristics of a decentralised infrastructure are:

1. Data centres and networking hubs with smaller transactional capacity and large storage capacity in Belgrade and few other selected sites
2. Local servers at each institutions with transactional capacities for the local operations
3. Wide Area Network with sufficient bandwidth for daily uploads of the transactions and for distribution of master data
4. Enterprise Service Bus or similar middleware that facilitates the interoperability and information exchange internal and external systems and which enables the daily distribution of required information.

This decentralised infrastructure needs WAN with lower capacity and reliability than the centralised infrastructure thus less investments, but requires more local servers and local system administration personnel.

The decision between the two architecture models depend on the long term financing power of the Ministry.

D.1.1. DATA-CENTRES AND NETWORKING HUBS IN BELGRADE, NOVI SAD, KRAGUJEVAC AND NIŠ

It is expected that many business processes in the justice sector will evolve and undergo modernization and optimization in the future. To allow better flexibility and easier accommodation to organizational changes and changes in the legal-framework, all systems should be designed and implemented based on centralized Service Oriented Architecture (SOA), with loosely-integrated set of software services, fully owned by the MoJPA.

Centralized, SOA-based architecture, if implemented properly, offers many business-critical advantages:

1. Consolidation and easier maintenance of hardware and network equipment
2. Easier manageability and deployment of applications
3. Better scalability and easier capacity growth
4. Easier virtualization – less physical servers and electrical power are required to provide the same level of services, than it is the case with distributed architecture (e.g. servers in each court).
5. Increased security – physical, network and application/database security in centralized environment it is much better than in geographically distributed architecture.
6. Information aggregation from several systems while maintaining their individual autonomy and self-governance.
7. Easier data exchange between both internal and external systems

At the same time, centralized architecture brings some challenges:

1. Possible single point of failure could cause nation-wide business continuity problems which brings the need to give considerations to building in redundancy into the architecture
2. Heavy network congestion at the central locations in peak periods
3. Risk of large-scale data loss/corruption in central database

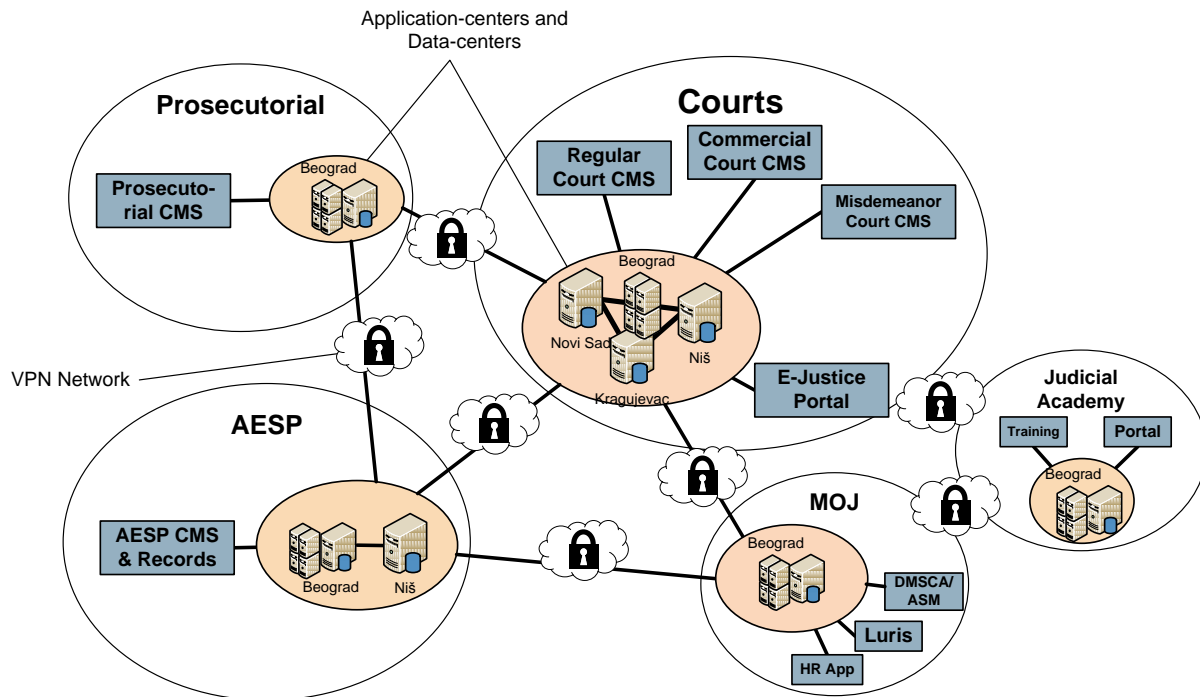
However, performance and reliability of the business critical applications depend not only on performance of the application servers and database servers, but also on the endpoint network bandwidths, reliability of power network, and cooling capacity of the air-conditioning systems deployed.

All these challenges have to be addressed through fault-tolerance and high-availability mechanisms implemented at hardware, software, and power and network level. With these mechanisms properly implemented, and well balanced, centralized architecture can provide extremely high level of availability (e.g. 99.99% or even 99.999% uptime) for all systems and services.

The following diagram depicts the recommended high level architecture vision of the justice sector systems in case of first alternative (with own data centres). In case of usage of e-Government cloud services as an alternative, the high level architecture diagram depends on the e-Government architecture.

For the second alternative, the logical topology of the network may be similar, but WAN connections require less bandwidth and local server environment contains the local database and application servers.

Logical diagram of the future E-Justice Systems



Power considerations: server-farms and supporting network equipment consume large amounts of electricity.. Simultaneously, such servers rarely operate on their peak performance (and only during standard business hours), so one of the critical procurement decision parameters should be performance per watt, and not simply raw performance. The MoJPA has two primary ways to decrease energy footprints and power costs of the data centres:

- Virtualization technologies - increasing performance per watt ratio through consolidation of many logical servers in single physical hardware
- Emphasis on “green” and power saving features when procuring servers.

D.1.2. WIDE AREA NETWORK

As stated earlier, availability, security and performance of the web-based applications built upon SOA architecture critically depend on the availability, reliability, security and bandwidth of the WAN network at the end-user locations. This puts tremendous importance on Wide Area Networking that has to be strengthened and improved beyond its current state, while strictly implementing relevant SRPS/ISO 2700x standards regulating information security.

While the existing WAN and LAN infrastructure is well developed at many sites, the largest gaps to bridge in the future are:

1. Incorporation of Misdemeanour Courts into courts Wide Area Network, and provision of essential LAN infrastructure in some of the court buildings;
2. Incorporation of Prosecutor's offices into judicial Wide Area Network, and provision of essential LAN infrastructure in some of the PO buildings, especially in case of building not shared with courts. In case of shared buildings, WAN development is not only technical, but procedural issue as well;
3. Provision of optical links to locations that are currently using Wireless and ADSL links.
4. Implementation of fail-over and redundant link capabilities at key locations, determined by the MoJPA

5. Implementation of SRPS/ISO standards regulating information security.

The recommended logical topology of the Wide Area Networks should adhere to centralized, star topology with segregated data centres and network-hub locations for each of the following entities:

1. Courts WAN – divided into virtual networks (VPNs) for different types of courts

Central hub location: Supreme Court of Cassation, Nemanjina 9, Belgrade

2. Prosecutors' WAN

Central hub location: Palata pravde, Savska 17, Belgrade

3. AEPS WAN;

Central hub location: Central Prison, Bačvanska, Belgrade

4. Judicial Academy WAN

Central hub location: Judicial Academy, Karadjordjeva 48, Belgrade

5. MoJPA WAN

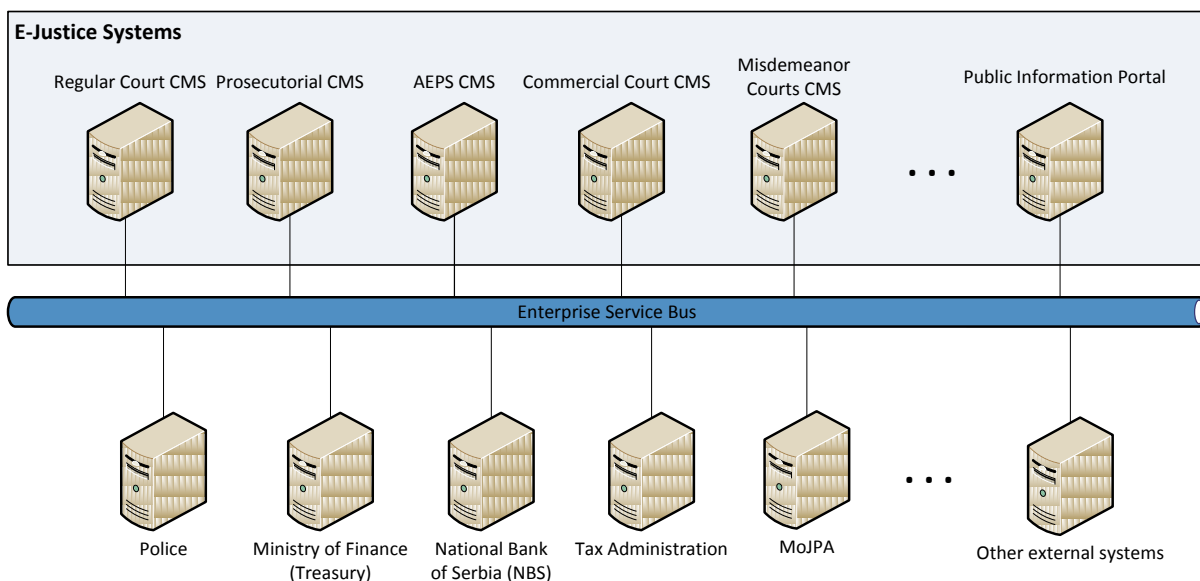
Central hub location: Ministry of Justice and Public Administration, Nemanjina 22-26, Belgrade

The Ministry of Justice and Public Administration and its directorates are formally part of the Serbian Government, and for that reason, the Administration for joint services of the republic bodies (UZZPRO) should continue to be responsible for provision and maintenance of LAN/WAN services, e-mail and DNS in the future for the Government part of duties. Judicial duties of the Ministry should be covered by the Justice WAN services.

Whenever UZZPRO WAN/LAN services may be extended to other justice sector institutions, this possibility should be investigated.

D.1.3. ENTERPRISE SERVICE BUS

With many information systems under implementation within the Serbian Justice Sector, there will be an increased need of exchange of information. This information exchange will occur both internally (between Ministry of Justice and Public Administration, courts, prosecutorial offices, prisons, information portals etc.) and with external organizations such as Police, Tax Administration, Treasury, Tax Administration, National Bank of Serbia etc.



As the number of required bidirectional links between communicating systems can be as high as $N*(N-1)/2$ where N is the number of communicating systems, it is not cost effective nor efficient to implement and maintain separate communication channels and data exchange protocols between all systems involved.

In addition to cost effectiveness, differences in technologies, platforms, exchange data formats and access control mechanisms between various systems may require a middleware, most likely in the form of Enterprise Service Bus, which would support service-level architecture (SOA) and seamless data sharing between different systems and different platforms, compliant with relevant SRPS/ISO standards for information security.

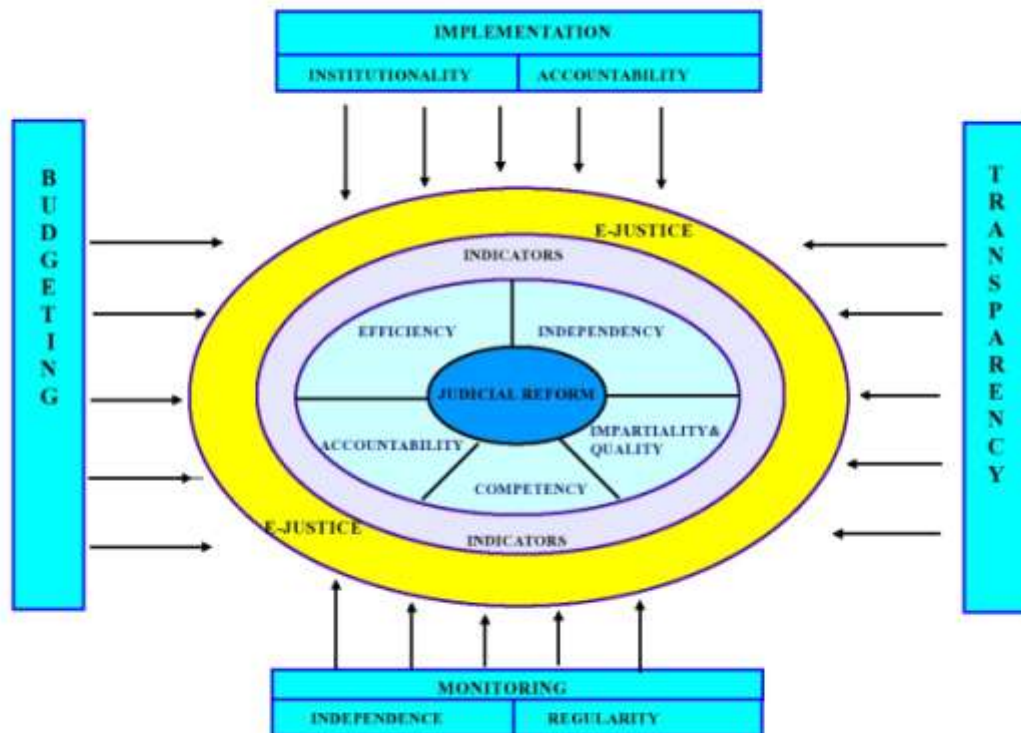
The enterprise service bus should allow each particular system involved, to communicate with the enterprise service bus in the same way, while the ESB middleware handles the actual translating to individual communication mechanism and data formats needed for the specific endpoint. This means that each system vendor will have to implement only single functionality to “talk” with the enterprise service bus, using a single messaging scheme (data namespace/format), while the bus middleware seamlessly and asynchronously translates that scheme so the endpoint system can receive it and understand it.

D.2. ORGANIZATIONAL VISION

With the increase of investments in the Information Technology and heavier reliance on Information Technology in the everyday operations of the Serbian Justice sector the need for better organization of ICT had become evident. The current ICT organization is fragmented, and although the Ministry has an e-Justice unit, but mainly because of its small staff it cannot fulfill the role of a modern ICT organization.

The new national judicial reform strategy “Judicial Reform 2013-2018” envisions an e-Justice layer encompassing the whole justice sector.

ANNEX 1



In the “Judicial Reform 2013-2018” document, ICT is not taking its due part and importance, although it is mentioned on several instances. The new “Judicial Reform 2013-2018” defines „e-Justice“ as: „Establishment of the system which providing opportunity for searching comprehensive and periodically updated databases through numerous criteria. Enable direct access to the court proceedings electronically. E-Justice improves financial efficiency of the court proceedings, as well as citizens' access to justice.”

This Judicial ICT Strategy Report envisions a broader definition of the e-Justice: "e-Justice is the new concept of how a justice system should operate, where ALL information and services are by default and according to legal rules made available to all interested parties, according to their authorization, in a virtual fashion, in electronic form, and only BY EXCEPTION are certain services and information excluded from this rule, based on a well-documented justification." (Here the word 'virtual' means that the user can be physically anywhere.)

The new ICT unit or organization for the whole sector should be instrumental in preparing the conditions for the introduction of such e-Justice principles and operations throughout the sector.

To achieve the recommended goals of the Justice Sector ICT strategy – and thus contributing to the overall Justice Reform, a strong centralized management is needed to implement components of the e-Justice environment. Moreover new technologies (especially centralized application systems, widely used networking capacities, digitalization of documents, information security challenges and knowledge sharing applications) require a strong central unit or organization to define the rules, internal standards, roadmaps for development and to maintain a uniform high level services for each Justice Institutions and end-users.

This centralised ICT unit or organization must possess the required authority over the local ICT operations of the individual institutions. Its position within the Justice sector should be strengthened. The ICT unit or organization should be centrally organized with responsibilities for:

- Strategy and Monitoring,

- Execution and Development and
- Support and Coordination.

D.2.1. STRATEGY AND MONITORING

This functional segment is concerned with monitoring the progress in the fulfillment of the current strategy as well as with the definition of the future strategy for the ICT in the Justice sector. The Strategy and Monitoring segment should have proper mechanisms to take into consideration the requirements of the higher level institutions including the Ministry of Justice and Public Administration, High Judicial Council, Supreme Court of Cassation, State Prosecutors Council, Republic Prosecution Office, Administration for execution of Penitentiary Sanctions and Directorate for Management of Seized and Confiscated Assets.

D.2.2. EXECUTION AND DEVELOPMENT

This functional segment should deal with the execution of the strategic actions, management of ongoing projects and development of the ICT procedures, practices and infrastructure within the judicial sector.

The Execution and Development segment should have the following functional areas:

- Project Management
- Business analysis,
- System architecture design,
- Risk analysis and Security design,
- Service design and management).

D.2.3. SUPPORT AND COORDINATION

This functional segment would be basically a contact center (Service Desk) combined with first level technical support of the local institutions. Whenever issues may not be resolved at the local institutions, problems are to be escalated to the Service Desk. The duties would be in dealing with the everyday practical issues of the Justice sector employees when working with the ICT systems and equipment to handling the e-Justice knowledge database and quickly finding the right answers to asked questions.

The Support and Coordination segment should have the following functional areas:

- Service Desk
- Second line ICT Support

The Service Desk provides all defined services to the employees of the Justice sector. The ICT Support deals with the everyday working challenges of the employees and resolves the practical issues that arise.

D.3. GOVERNANCE VISION

The purpose of IT governance is to make decisions that ensure IT investments help achieve Justice Sector goals. In order to succeed in that, IT governance shall focus on matters of key strategic value: basic principles, investment priorities, infrastructure and architecture standards and critical application choices; and provide both an environment for collecting viewpoints and data, and process for making decisions.

Within the Justice Sector in Serbia, where such strategic reliance is placed on the ICT function developing and delivering complex systems to support both Justice Sector and society expectations, The successful alignment

of IT and the business is more and more critical and mature IT governance practices enhance the ability of IT to deliver strategic initiatives based on efficiency, control and value.

Either the practice of IT governance has committed to a constructive link between higher levels on participation in IT and better IT effectiveness; there are emerging issues related to the IT organization, in order to follow the IT within the Justice Sector which moves its services and responsibilities, from distributed toward central ones in which users can access services that integrate many different resources. The competence of connecting the right information will become essential to effective IT leadership. As more technology decisions request for some kind of shared input and decision making, and especially as technologies get ever more deeply imbedded in the everyday life of the Justice Sector, IT management will have to improve further their ability to articulate the strategic implications and interests that governance participants should consider.

The IT continues to see ever increasing challenges from the business in the delivery of services and systems. The context of this delivery and the environment in which the IT operates is also continuously changing. Changing regulatory requirements, management of more and more complex cases and a diverse group of key stakeholders whose expectations need to be managed all conspire to increase the challenge. In the face of these significant challenges, IT governance would bring clarity around the responsibility, authority and communication and reporting flows which enhance decision making. Accompanying policies, processes, standards and control mechanisms enable Justice Sector staff to carry out their roles and responsibilities. Effective IT governance is therefore a key strategic enabler for evolution and success and helps to achieve the fusion of IT and the business. However, to achieve these ambitions it must be addressed in the context of the wider business governance and be strategically aligned through the value chain.

The used framework for assessing and presenting the future vision of IT operations is the COBIT framework. COBIT's process maturity model assigns a maturity level (from 0 to 5) to each IT processes of the framework which covers in theory the complete operations of an IT organization.

COBIT divides the full domain of IT into 4 domains:

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

Each of them consist some process areas. For each process area, control objectives and good practices are formulated together with detailed methods how to assess the IT situation of an organization.

Within these groups the individual processes were assessed from maturity viewpoint. This maturity assessment gives an overall picture on the whole justice sector for both current and the future state of the IT Governance.

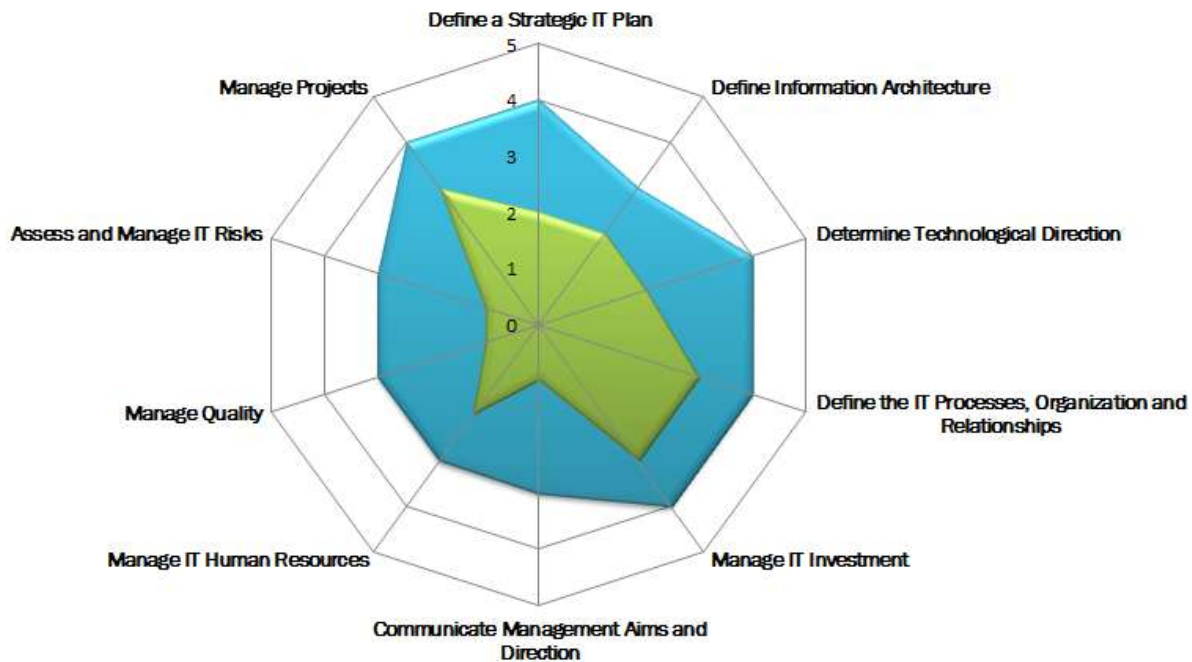
D.3.1. PLAN AND ORGANISE

The processes and most important characteristics for the Consultants' recommended TO-BE maturity levels within the "Plan and Organize" process group are the following:

ID	Process	Description	Maturity Level Description	Maturity level
PO1	Define a Strategic IT Plan	Processes to identify strategic requirement of the business and align IT plans to fulfil these requirements	Management is regularly monitoring the strategy planning process. IT and business strategies are aligned via well-established organizational mechanisms	4
PO2	Define Information Architecture	Process is to enable IT being agile to provide reliable and consistent information and to integrate applications with business processes.	Data Administrator position is established. There are standardized processes to define data, their relationship. Documented data flows exist.	3
PO3	Determine Technological Direction	Processes to establish technology standards and define technology plans to support business.	IT staff members have the skills to develop technology infrastructure plan. Plan is regularly revised, migration plans are created.	4

ID	Process	Description	Maturity Level Description	Maturity level
P04	Define the IT Processes, Organization and Relationships	Processes to define roles and responsibilities within IT	IT organization proactively responds to changes. Measurable metrics exist for the IT processes. Skill inventories are available	4
P05	Manage IT Investment	Processes to define, accept and control financial resources	Budget variances are identified and resolved. Formal cost analysis is performed covering direct and indirect costs over total life cycle.	4
P06	Communicate Management Aims and Direction	Ongoing communication to articulate mission, service objectives, policies, projects	Complete framework for policies, procedures is developed and communicated. Techniques to promote security awareness have been standardized	3
P07	Manage IT Human Resources	Processes to continuously acquire and maintain competent workforce to deliver IT services to the business.	Human resource processes are defined and documented. Formal training plan and rotation programmer is established	3
P08	Manage Quality	Processes to maintain a quality management system by providing clear quality requirements, monitoring quality measures.	A defined quality management system is communicated. Education and training programs are held. Quality satisfaction programs are conducted.	3
P09	Assess and Manage IT Risks	Processes to create and maintain risk management framework, to analyze and mitigate risks.	Organization wide risk management policy defined when and how to conduct risk assessment	3
P010	Manage Projects	Processes to ensure project coordination, planning, resource allocation, deliverable approval, project risk management.	Management requires formal and standardized project metrics. IT management implements a project organization structure. Relevant project management training is held.	4

The overall summary of the current (green) and Consultants' recommended future (blue) maturity levels can be seen on the following diagram:

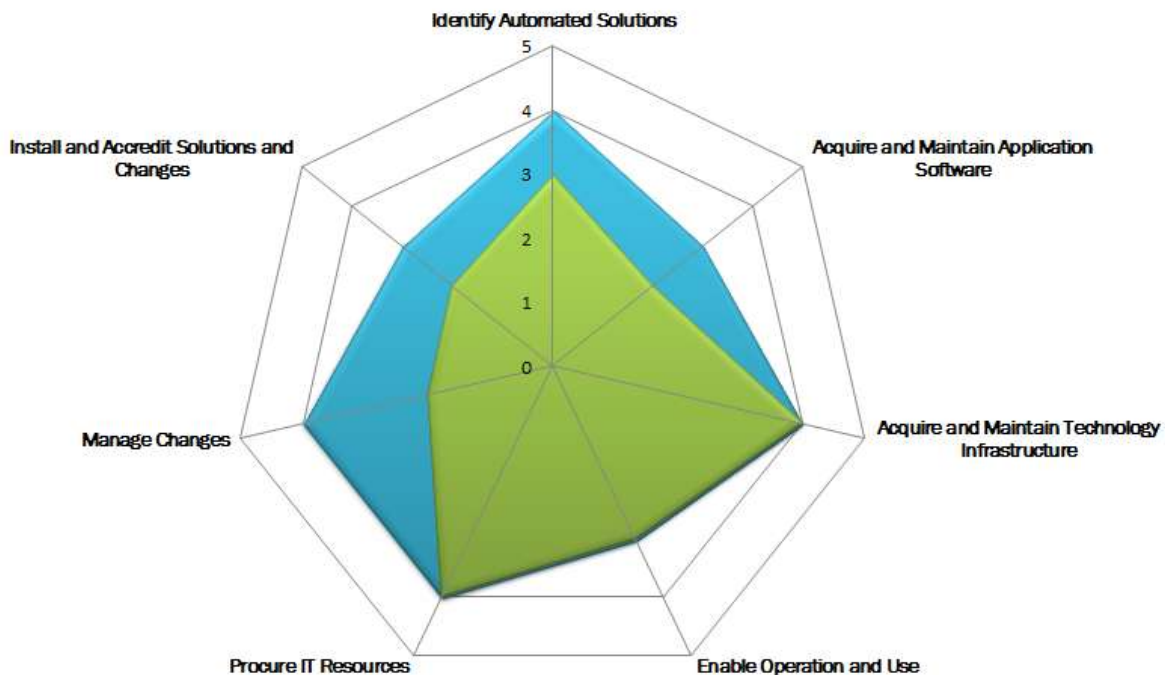


D.3.2. ACQUIRE AND IMPLEMENT

The processes and most important characteristics for the Consultants' recommended TO-BE maturity levels within the "Assessment of Acquire and Implement" process group are the following:

ID	Process	Description	Maturity Description	Maturity Level
AI1	Identify Automated Solutions	Processes to identify business requirements, to consider alternatives and to execute risk analysis prior to solution acquisition	There is an established methodology for identification and assessment of IT solutions. Cost benefit analysis is part of evaluation of alternatives	4
AI2	Acquire and Maintain Application Software	Processes to specify design and develop applications.	A clear defined process exists for acquisition and maintenance of application software.	3
AI3	Acquire and Maintain Technology Infrastructure	Processes to plan and execute acquisition and maintenance	IT infrastructure adequately supports business applications. Process is well organized.	4
AI4	Enable Operation and Use	Processes to produce proper documentation and manuals for users and to provide trainings for end users and operators alike	There is a clearly defined framework for user documentation, operation manuals and training materials. Corrections to documentation are made on a reactive basis. Business and user training is planned and scheduled	3
AI5	Procure IT Resources	Procedures to procure hardware, software and services	There are standards for all IT procurement processes. Reporting is continuous on IT acquisition processes.	4
AI6	Manage Changes	Procedures to formally manage and control all patches, version changes in the productive environments	Change management process is strictly enforced. All changes are subject to impact assessment. Changes are fully documented.	4
AI7	Install and Accreditate Solutions and Changes	Procedures to ensure proper testing, definition of rollout criteria and release planning	A formal methodology exists for installation, migration and verification.	3

The overall summary of the current (green) and Consultants' recommended future (blue) maturity levels can be seen on the following diagram:

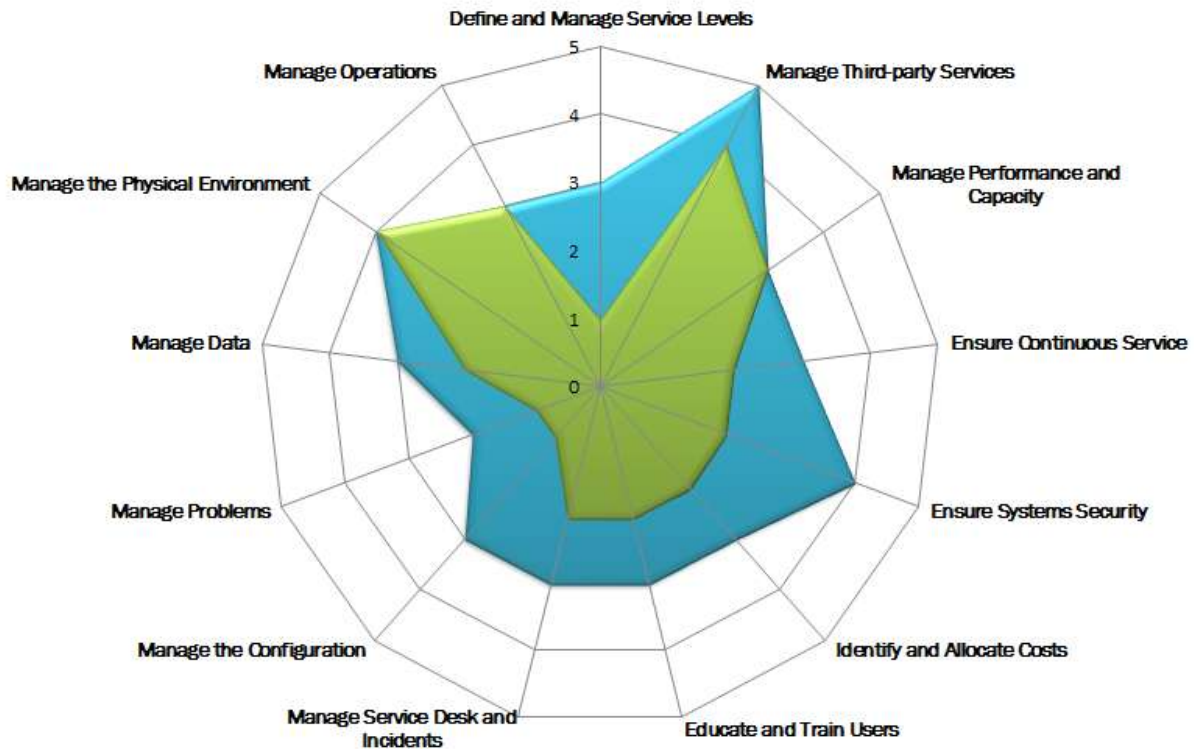


D.3.3. DELIVER AND SUPPORT

The processes and most important characteristics for the Consultants' recommended TO-BE maturity levels within the "Assessment of Deliver and Support" process group are the following:

ID	Process	Description	Maturity Level Description	Maturity Level
DS1	Define and Manage Service Levels	Procedures to define, monitor and communicate service levels between IT and business users	Service Levels Agreement process is implemented with checkpoint for reassessing service levels	3
DS2	Manage Third-party Services	Procedures to define roles, responsibilities in third-party agreements	Contracts signed with third parties are periodically reviewed. Comprehensive reporting of service level achievement is linked to third-party compensation.	5
DS3	Manage Performance and Capacity	Procedures to review and forecast performance and capacities of IT resources	Performance and capacity requirements are defined throughout the system life cycles. Future capacity needs are modelled	3
DS4	Ensure Continuous Service	Procedures to develop and test IT continuity plans, to provide offsite backup storage	Accountability for continuous service is assigned. IT continuity plans are documented and tested. High availability components and redundancy is applied	3
DS5	Ensure Systems Security	Procedures to establish IT security roles, policies and to perform security monitoring and to implement actions	IT security risk and impact analysis is performed. User identification, authentication is standardized. IT security training is conducted in IT and in business.	4
DS6	Identify and Allocate Costs	Procedures to measure and allocate IT costs together with business involvement	There is a defined and documented IT services cost model.	3
DS7	Educate and Train Users	Processes to identify training needs, to train and to measure results	A training and education program is instituted and communicated. Training process is standardized. Budgets are established to support trainings	3
DS8	Manage Service Desk and Incidents	Processes to effectively respond user queries and problems	There is a service desk with standardized procedures. Queries and incidents are tracked. Timely response is not measured	3
DS9	Manage the Configuration	Processes to keep track of hardware and software configurations and their changes	Configuration management processes are documented and standardized. There are tools to gather and store configuration information.	3
DS10	Manage Problems	Processes to identify, analyze and resolve problems	There is a problem resolution process with dedicated individuals. Information is shared amongst staff	2
DS11	Manage Data	Processes to maintain and recover data and to ensure data security	Responsibility for data management is established. Data management procedures are formalized	3
DS12	Manage the Physical Environment	Processes to manage facilities, physical access and monitor environmental factors	Environmental and physical security requirements are documented. Access is strictly controlled and monitored.	4
DS13	Manage Operations	Processes to define operating policies, scheduled processing, monitoring performance and maintenance of equipment	Need for operations management is understood. Repeatable functions are formally defined. Completed task results are recorded and reported.	3

The overall summary of the current (green) and Consultants' recommended future (blue) maturity levels can be seen on the following diagram:



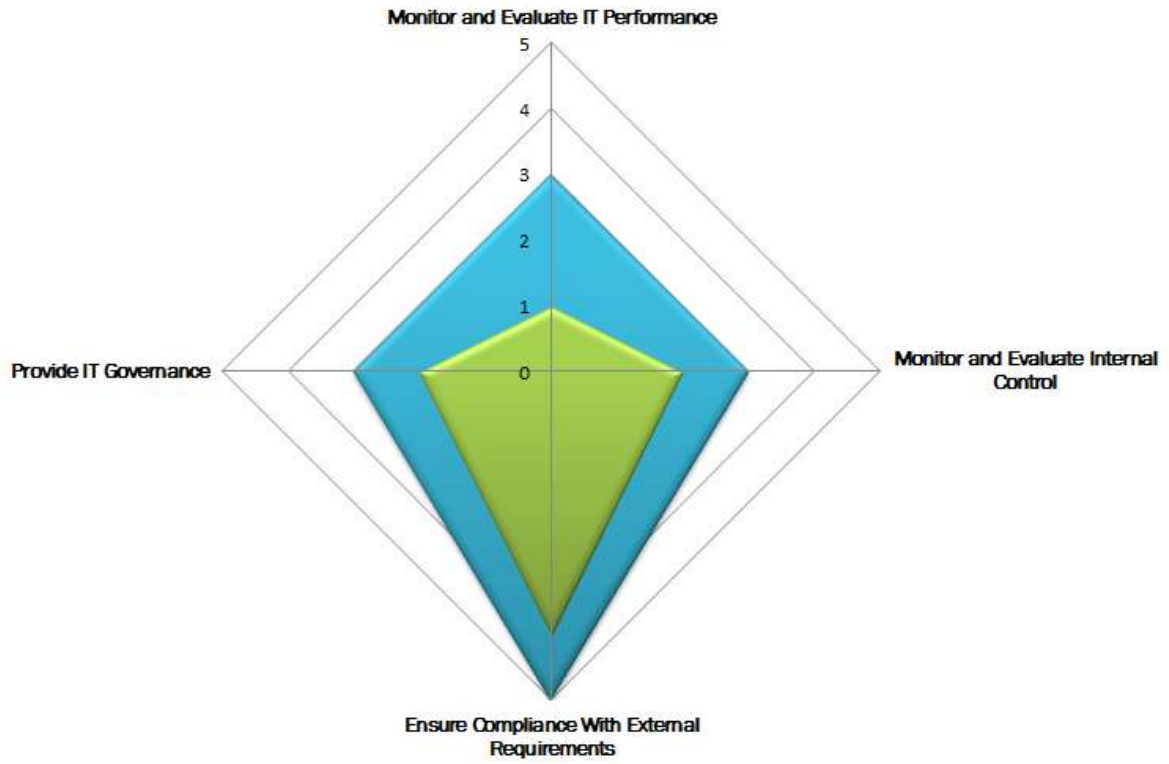
The major theme of the “Assessment of Monitor and Evaluate” group of processes is the existence and evaluation of controls to manage and govern the IT operations to satisfy the business. IT controls are implemented mechanisms to prevent, detect and correct undesired events or their effects.

D.3.4. MONITOR AND EVALUATE

The processes and most important characteristics for the Consultants' recommended TO-BE maturity levels within the “Assessment of Monitor and Evaluate” process group are the following:

ID	Process	Description	Maturity Level Description	Maturity Level
ME1	Monitor and Evaluate IT Performance	Processes to define, measure and report indicators and act upon deviations	Management implements standard monitoring process. Training programs are implemented. Tools for monitoring IT processes and service levels are implemented.	3
ME2	Monitor and Evaluate Internal Control	Processes to establish, monitor and report controls and control exceptions	Policies and procedures are developed for assessing and reporting internal controls. Self-assessment process is defined.	3
ME3	Ensure Compliance With External Requirements	Processes to identify, evaluate compliance with laws, regulations, contractual obligations and to respond in order to achieve compliance	There is a single central function that provides guideline and control over compliance. Self-assessment process is established.	5
ME4	Provide IT Governance	Processes to define organizational structures, processes, leadership and responsibilities to ensure IT investments and operations are aligned with business objectives	Set of IT governance indicators are developed. Management communicates standardized procedures. IT goals are clearly set and communicated.	3

The overall summary of the current (green) and Consultants' recommended future (blue) maturity levels can be seen on the following diagram:



E. DETAILS OF STRATEGIC DIRECTIONS

E.1. ESTABLISH PROFESSIONAL, SERVICE ORIENTED ORGANIZATION

E.1.1. RELEVANT PARTS OF DIAGNOSIS

Normal functioning of the Ministry and the judicial system, including performance of its core functions, is supported by units providing IT services. In the Ministry this is the Unit for e-Justice. The Unit in the Ministry is directly responsible for the implementation of the ICT projects within the whole Justice Sector. Other institutions have similar IT units. The main task of these units is the management (creation, deployment, maintenance and development) in the provision of IT services. Although some of the courts and institutions have their own IT-related projects, they are all in sync with the plan of the Ministry.

Currently the Justice Sector employs 338 ICT staff which is approximately 2% of total judiciary staff, however the law allows for more ICT employees to be hired. Additionally outside staff is used through maintenance and project contracts for different aspects of the ICT system development in the judiciary.

In the recent period there have been many changes introduced in the sector in regards to the ICT systems. This has produced some level of strain on the already existing systems and the habits of the employees. Proper change management and training had been initiated and is still ongoing, but more technical assistance, change management and training expertise is required in this filed.

It is very important to note that the whole Justice Sector is currently undergoing reorganisation and that some changes have not been completed yet. Organisational transitions tend to have the effect of reduced retention as well as reduced productivity of the employees.

Also there is a lack of modern, sector wide, human resource management tools, which can greatly benefit all stakeholders into managing the development of the employees and tracking of the individual as well as the overall progress.

Another current issue in the turnover of staff is that there are no legal instruments which would allow the stakeholders to hold the trained ICT staff and often it happens after receiving some experience and some training that the people leave their positions within judiciary.

E.1.2. INTERNATIONAL TRENDS AND EU PRACTICE

The Austrian experience of ICT in the judiciary is a model for some countries in the Balkans region candidates for EU accession. Their experience shows that a centralised organisation for managing all of the ICT needs and employees in the judiciary is an excellent solution. The Austrian central judiciary ICT service agency is called the Federal Computing Center and Consultants believe that it would be a good **role model** for the Serbian Justice ICT independently on its organisational position.

Since the beginning of the eighties of the last century, Austria's judiciary system has built up a comprehensive IT network. This network supports the nation-wide use of IT applications. All courts, offices of public prosecution, prisons and the Federal Ministry of Justice and Public Administration can cooperate via the interface at the Federal Computing Center, where all judicial applications are supported. The Federal Computing Center is also responsible for communications with the other federal ministries and service units, as well as, ultimately, all citizens.¹

¹ THE AUSTRIAN JUDICIAL SYSTEM (Institutions - Agencies - Services, Vienna, January 2009, Federal Ministry of Justice, http://www.justiz.gv.at/internet/file/8ab4ac8322985dd501229ce2e2d80091.en.0/die_justiz_eng_05.09.pdf)

E.1.3. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- Loyal IT staff, popularity of public administration jobs leads to longer-term employment of judiciary IT staff
- Enthusiastic and competent training and IT staff in the Judicial Academy

Weaknesses

- ICT staff numbers too low, no specialization of ICT roles
- No special selection and testing of ICT staff in the hiring process
- In some Justice Sector institutions, salaries of ICT professionals are lower compared to other Justice Sector employees and the private sector
- No developed career path for ICT employees
- IT operations are fragmented (staff, procurement, maintenance)
- Lack of established performance measurement system for ICT

Opportunities

- Availability of international standards for regulation of various aspects of ICT developments and operations
- Access to qualified ICT staff on the local IT market

Threats

- Perpetual changes in the institutional framework of the Justice Sector
- Talented ICT professionals, well-trained experts / trainers may be drawn away to the private sector with a promise of better salaries and career paths

E.1.4. GOALS RELATED TO THE AREA

Mid-level ICT goals

- ICT staff is motivated and educated to ensure staff retention and required competences
- User requests are addressed and served within definite time limits
- Standardised and optimised IT operational procedures

E.2. ESTABLISH CENTRAL, WELL STRUCTURED, SECTOR WIDE ICT ORGANIZATION

E.2.1. RELEVANT PARTS OF DIAGNOSIS

During the past decade with the aid of different donors the ICT sector of the Serbian judiciary has seen investments well over 10 million euro and with annual ICT budget of the Ministry in the range of 2,5-3 million Euros. The investments mainly went into infrastructure and system development, as well as some institutional building services. However the status as recorded in the Diagnostic report shows that the organization of the ICT sector in the judiciary is heavily fragmented, without clearly stated rules, authorities and works according to an old

strategy, which had run its course. The head of the organization is located in the Ministry of Justice and Public Administration and numbers 5 people. The rest of the ICT staff is dispersed throughout the institutions in the whole sector and answers primarily to the heads of the respective institutions.

Protecting and more importantly sustaining these investments in the modernization of the Serbian justice sector requires a serious, well-organized body, with sufficient authority to manage the existing and future ICT needs of the judicial institutions.

The reforms in the Serbian justice sector are still ongoing, the new reform strategy is formulated, and therefore the ICT structure must be strengthened in order to support the new system.

The diagnostic work of this project has shown that the current organization in the ICT area is not able to meet all of the requirements with sufficient coordination, efficiency, authority and level of quality, so not all ICT needs are being served in an optimal fashion.

E.2.2. INTERNATIONAL TRENDS AND EU PRACTICE

The computerisation of the judiciary in Europe is a trend that has been going on since the 80's of the last century. There are plentiful examples of fully computerised and IT-supported judicial systems. Most of these countries have specialised ICT organizations, in one form or another, in order to be able to deal with the growing IT needs of the modern judicial systems; this is evolving today into a paradigm, under the name e-justice.

The pan-European high courts, such as the ECJ and ECHR, have also well-developed ICT organizations, and are building on the capability to further improve the interconnections between the European justice systems. As Serbia is on the path of becoming a EU member state, it is a clear requirement that its justice system is harmonized with the EU justice system, so that EU accession can go more smoothly (justice area, i.e. rule of law, will be one of the first to start negotiating on, once the formal accession negotiations start). The harmonization of the justice system also means harmonization of the ICT systems supporting the Serbian judiciary.

In several European Countries (for example the "Bundesrechnungszentrum" of Austria or the "Central Office for Administrative and electronic Public Services") there is an even more centralised ICT service provider on governmental level responsible for various services. There are examples for being a governmental agency or for being an agency in some form of public-private partnership.

E.2.3. GOALS RELATED TO THE AREA

Mid level ICT goals:

- Standardised and optimized operational processes
- Having standardized application environment
- Unified project management procedures and unit responsible for sector-wide projects
- Availability of a Central Registry of all sectorial ICT systems
- ICT staff is motivated and educated to ensure staff retention and required competences
- Knowledge and practices are shared, easy to find, uniformly interpreted and constantly applied

E.2.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- State of the art Case Management systems at some institutions

- Loyal IT staff, popularity of public administration jobs leads to longer-term employment of judiciary IT staff
- Experience of ICT staff in operation of justice systems
- Existing coordination of ICT development efforts

Weaknesses

- ICT staff numbers too low, no specialization of ICT roles
- No special selection and testing of ICT staff in the hiring process
- No developed career path for ICT employees
- IT operations are fragmented (staff, procurement, maintenance)

Opportunities

- ICT Strategy is under preparation to give a framework to and coordinate development efforts
- Availability of national and international standards for regulation of various aspects of ICT developments and operations
- Access to qualified ICT staff on the local IT market

Threats

- Perpetual changes in the institutional framework of the Justice Sector
- Talented ICT professionals, well-trained experts / trainers may be drawn away to the private sector with a promise of better salaries and career paths

E.3. ENSURE SUSTAINABILITY THROUGH “SERVICE LIFE CYCLE MANAGEMENT

E.3.1. RELEVANT PARTS OF DIAGNOSIS

The diagnosis related to the ICT systems sustainability is mainly in the “ICT Process Maturity assessment” The key findings are the following:

- There are no defined, measured and evaluated service levels towards end-users (maturity level of “DS1 Define and Manager Service Levels” process area is currently 1)
- There is no single centralised inventory on the ICT assets what inhibits the careful planning of changes (maturity level of “DS9 Manage the Configuration” process area is currently 1)

In general ,the most common factor for the failure of newly created ICT systems does not come from a technical background, but in fact it comes from the non-usage of the new systems by a minimal, critical mass of users; thus not allowing the system to actually become truly alive.

In this transitional period for the country, most of the new equipment and systems needed for proper functioning of the various institutions are procured by utilising donor provided funds either as grants, co-financing schemes or long term credits. This leads to procurement, design and delivery of highly complex and expensive ICT systems that support the needed functionalities by the various governmental institutions including the Justice Sector.

Additionally any kind of change in institutions that have long traditions, like the ones in the judiciary can take a lot of time, effort and finances. For example, changing the people’s long acquired habits when moving from a paper to an electronic document management system has proven to be hard and time consuming, even unsuccessful in some instances.

Another factor is the quality of the vertical communication within the institutions where the major challenges are that the heads of the institutions do not truly know the needs of the employees and on the other hand the employees do not really understand the bigger picture of their daily duties so their motivation is low or even they practice their duties in a wrong manner.

So what happens in real life is that the various institutions get advanced and modern tools in the form of ICT systems, but without the further finances and the additional manpower to use and sustain those same systems. Very often the existing employees get overburdened with double or triple duties for prolonged periods of time so they tend to neglect the new ICT systems in favour of paper based functioning. And it is then when the newly created ICT systems die without having truly lived.

E.3.2. INTERNATIONAL TRENDS AND EU PRACTICE

Before entering in any type of venture, and more specifically design and development of ICT systems to support the Judiciary it is a common practice in the EU countries to have a long-term strategy and a medium and short term action plan developed. The strategy sets out the directions and the high level goals while the plan deals with the practical aspects of the implementation, impact and the future sustainability of the newly planned ICT systems. Also the strategy needs to be strongly justified before the higher-level bodies in the judiciary and accepted at the highest level not just in the line ministry but also in the judicial institutions. It is very important to stress the independence of the judicial institutions in the modern society as one of the pillars of the modern countries.

The estimation of the Total Cost of Ownership is always an important part of any strategic planning and supports the justification and the decision-making. It gives the institutions and the government idea of how much does the new ICT system cost in terms of services, supplies, and human resources. And that is not just for the planning, development and the rollout, but also to be further maintained in the future. Beginning of development of any type of new system or introduction of change in an existing system without a previous professionally done feasibility study is hardly ever the practice in the EU countries. The TCO study also allows for future budget planning in the Justice sector in regards to human resources, system maintenance and updates.

Another important aspect to be considered is the change management, as the harmonization of the Serbian Justice system to the EU Justice system requires transitional changes that need to be closely managed. Change management practices vary from case to case, but a generally adopted method is the Change Acceleration Process Model (CAP Model), which consists of 7 levels of change management:

1. Leading change – Devoted and loyal leadership throughout the change is crucial for the success
2. Creating a shared need – The need for change must outweigh the resistance to change
3. Shaping a vision – Clear and legitimate vision of the targeted state must be communicated to the involved parties
4. Mobilising commitment – Execute the change, have “early adopters” of the new system act as ambassadors for change
5. Making changes last – Use experience and best practices from the successful pilots in the further roll-outs
6. Monitoring process – Measure the progress, set benchmarks, indicators and milestones.
7. Changing systems and structures - Hiring & staffing, IT systems, training & development, resource allocation, organizational design needs to be changed to support the new system.

Next to the strategy and action plan there should always be a change management plan.

E.3.3. GOALS RELATED TO THE AREA

Mid level ICT goals:

- Availability of a Central Registry all IT systems of the Sector
- Requests towards IT are registered and tracked by uniform IT application
- Legal professionals and court administration is knowledgeable on effective use of ICT
- Budget is in balance with operational costs
- Improved financial planning and cost control
- User requests are addressed and served within definite time limits
- Total costs of ownership is calculated at investment decisions

E.3.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- Experience of ICT staff in operation of judicial systems

Weaknesses

- No separate ICT infrastructure and ICT staff for prosecution offices
- ICT staff numbers too low, no specialization of ICT roles
- Lack of "user participation" in development projects
- Ministry budget is heavily constrained
- Budget planning is constrained by governmental accounting rules, the budget structure is not reflecting all aspects of ICT costs

Opportunities

- Price of new technologies and unit price of some capacities (i.e. storage) are decreasing,
- Governmental contract with Microsoft to cover licences for Office products
- Availability of international standards for regulation of various aspects of ICT developments and operations

Threats

- Growing maintenance costs as a result of donor-funded ICT developments and purchases
- Growing budgetary pressure and expenditure cuts

E.4. ENSURE FULL GOVERNANCE THROUGH SERVICE PERFORMANCE MEASUREMENT

E.4.1. RELEVANT PARTS OF DIAGNOSIS

ICT performance measurement

ICT performance measurement is a key component of IT governance, thus major statements can be found in the "IT Operations Assessment" section of the Diagnostic Report. According the CoBIT maturity model used for assessment, an ICT process is on maturity level 4 (Managed and measurable) if "Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively". As a general statement about maturity, only a few ICT processes reached this maturity level, partly because of the lack of a consistent (performance) measurement system. The major statements of diagnosis were:

- Maturity of Communicate Management Aims and Directions (PO6) has currently Maturity level 1, partially because of well established performance measures do not exist, thus Management goals are not quantified.
- Manage Quality (PO8) evaluation states that there are basic quality measures, mostly about project costs and times, but there are no customer satisfaction surveys. The planned implementation is SRPS ISO/IEC 27000 system would define quality measures at least for ICT security related areas
- Manage Projects (PO10) evaluation states that there are no uniform project metrics for project implementation
- Maturity of Define and Manage Service Levels (DS1) is currently 1, mainly because of the lack of exact ICT service definitions and service level agreements
- Maturity of Manage Third Party Services (DS2) is at level 4 with clear service definitions and reporting obligations for the vendors, however actual payments are not linked to performance measures.
- According to evaluation of "Managing Performance and Capacity" (DS3), the maturity level is 3, which denotes some existing measures for technical capacities.
- Evaluation of "Monitor and Evaluate IT Performance" (ME1) was level 1, since the major ICT goals are not quantified, and only the most critical measurements are done.

E.4.2. INTERNATIONAL TRENDS AND EU PRACTICE

Most international methodologies and frameworks for ICT operations and governance cover performance aspects. Virtually all ICT units of organisations use measurement systems, especially if they have outsourcing contracts. The widespread application of ITIL framework for IT operations extensively relies on Service Level Agreements both between IT unit and the end-users and between IT unit and third party vendors. According to recent trends, technical ICT performance measures are generated from applications supporting operations, like Service Desk systems, Network surveillance systems, while soft measures are generated from Project Portfolio Management systems and HR systems.

Based on the general Balance Scorecard Methodology briefly described in the Methodology section of this Report, specialised IT Balanced Scorecard methods also exist and are being used by IT organisations.

Some Justice Sectors ICT strategies prepared during the recent years devote attention to ICT performance measurement and in some cases even specific measures or techniques are given. For example:

- Turkish Strategy Plan for 2010-2014 defines measures like "*Rate of e-signature, rate of procedures performed electronically. rate of renewed computers*"
- In the Ministry of Justice Digital Strategy document of the UK Ministry of Justice, performance measurement is also an important component: "Taking steps to measure performance and deliver real-time management information"².
- USA Department of Justice Information Technology Strategic Plan for 2010-2015 deals extensively with performance metrics as "*The IT dashboard provides Web-based access to IT investment-specific information such as the investment's description, awarded contracts, current and past performance measures*"³

Even if developing IT performance measurement is not a separate issue of these strategies, they are all emphasize the strong links between overall strategic goals and IT goals, the importance of quality and the role of governance in IT operations.

² Source: <http://open.justice.gov.uk/digital-strategy/>

³ Source: <http://www.justice.gov/jmd/ocio/2010itplan/10it-strategic-plan.pdf>

E.4.3. GOALS RELATED TO THE AREA

Mid-level ICT goals

- Availability of Methodology for Inspection/Quality Control
- No parallel projects are financed
- During implementation of ICT system parallel development of the same functionality is eliminated
- Full training and education history of judges and prosecutors is available for decision makers
- Process and team performances are measured and evaluated

E.4.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- State of the art Case Management systems at some institutions
- New Case Management systems are developed on same platform
- Experience of ICT staff in operation of judicial systems

Weaknesses

- Fragmented case management systems, 3 separate ongoing implementations (SAPS, SAPO, SAPA)
- Statistical ICT system capabilities are underdeveloped
- IT operations are fragmented (staff, procurement, maintenance)
- Lack of established performance measurement system for ICT

Opportunities

- Price of new technologies and unit price of some capacities (i.e. storage) are decreasing,
- Availability of international standards for regulation of various aspects of ICT developments and operations

Threats

- Talented ICT professionals, well-trained experts / trainers may be drawn away to the private sector with a promise of better salaries and career paths

E.5. INTRODUCE SERVICE HELP DESK TO PROVIDE SUPPORT

E.5.1. RELEVANT PARTS OF DIAGNOSIS

First line support is provided by vendors in case of major Case Management Systems, but there is no centralised Service Desk for all ICT related problems/requests. Handling ICT related problems is fragmented (maturity level of "DS8 Manage Service Desk and Incidents" process area is currently 2)

E.5.2. INTERNATIONAL TRENDS AND EU PRACTICE

The positive experience for public sector management that currently is in focus of the developed countries is the Nordic countries experience, namely Sweden, Norway, Denmark and Finland, specifically the establishment of professional Service Desks on sector level. The lesson that can be learned is that many of the public institu-

tions operations that are non-core for the judiciary, such as human resources, payroll, ICT are often outsourced to private companies. This has the effect of creation of more efficient and healthy public sector systems. Also sharing these services between the institutions had the effect of overall savings in the sector. The UK justice sector is also an example of this experience.

E.5.3. GOALS RELATED TO THE AREA

Mid level ICT goals:

- Availability of a Central Registry all IT systems of the Sector
- Requests towards IT are registered and tracked by uniform IT application
- Legal professionals and court administration is knowledgeable on effective use of ICT
- User requests are addressed and served within definite time limits

E.5.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- Experience of ICT staff in operation of judicial systems

Weaknesses

- ICT staff numbers too low, no specialization of ICT roles
- Lack of "user participation" in development projects

Opportunities

- Price of new technologies and unit price of some capacities (i.e. storage) are decreasing,
- Availability of international standards for regulation of various aspects of ICT developments and operations

Threats

- Growing budgetary pressure and expenditure cuts

E.6. ENSURE SUSTAINABILITY VIA PROPER FINANCIAL (BUDGET) MANAGEMENT

E.6.1. RELEVANT PARTS OF DIAGNOSIS

The diagnosis of the funding issues is partly included in ICT Spending and ICT Operations Assessment sections of the Diagnostic Report. The key findings are the following:

- Maturity of Identify Automated Solutions (AI1) process is currently 3, partly because when large implementation projects are defined, the long term costs (Total Cost of Ownership) are not determined and not considered when selecting form among options.
- High Judicial Council and State Prosecutors' Council are responsible for consolidating operational budgets of the relevant courts and prosecutor offices respectively, thus for ICT operational budgets as well.
- Ministry's ICT budget was increased nearly 20% over 2 years (2010-2012), which covers network development and operations, replacement of about 15-20% of end-user workstations across the whole

sector, sector-wide virus scanner maintenance, ICT staff trainings and some small-scale operational developments.

- In spite of the budgetary increase, the ICT is underfunded. This prohibits inter alia the homogenisation of end-user environment, and development of staff at the Ministry to establish an overall governance and regulatory role within the Justice sector.
- Large scale investment type projects are all funded by donor organisations in magnitude larger than the institution's own budgets.
- Operation and maintenance costs of software and hardware equipment implemented by donor-funded project encumbers the Ministry's and the Institutions' budgets.
- Donor organisations require careful preparation of projects more-and-more, covering business aspects and proof of alignment with strategy.
- Ministry's (and other institutions') ICT budget structure is aligned with the State budget structure and its granularity is not sufficient to substantiate outsourcing-related decisions, since ICT staff costs, infrastructure and utility costs are not covered.
- Currently budgeting is supported mainly by Excel sheets and a specialised budgeting application is being implemented at the High Judicial Council. Budget tracking is also mainly by MS Office applications.
- Administrative Efficiency Reform project implemented budget planning structure and framework but it is not used with full consistency.

E.6.2. INTERNATIONAL TRENDS AND EU PRACTICE

Budgeting and acquisition of funds for ICT cannot be strictly separated from general budgeting and fund-raising activities of the Sector. In the recent years – as in case other sectors – new budgeting approach have been applied in most developed countries⁴:

- budgeting process is linked to performance measures and identified gaps
- “budgeting by objectives” that is investment budget is strictly linked to development programs, and their components
- multi-year budget planning with forecasts to upcoming years

For states which are in a transitional period regarding the development of their administrative processes, this provides good possibilities to establish solid framework for acquisition of donor funds, since donor organisations only support investment type of expenditures.

Naturally the ICT budgeting process cannot be separated from the general budgeting processes, but ICT budget planning has its specialities which should be considered:

- Total Cost of Ownership approach to estimate and establish budgetary forecasts after implementation projects
- Cost/Benefit analyses when preparing the initial project requests
- Consideration of non-traditional ICT costs, like staff expenses, yields of improved productivity, cost of facilities and utilities
- economies of scale considerations
- cost of technological diversity versus homogeneous technology environment
- outsourcing opportunities

In practice, the above aspects have the following direct consequence of ICT budgeting:

- Investments are clearly lined to strategic initiatives

⁴ Source: http://siteresources.worldbank.org/INTLAWJUSTICE/Resources/LDWP3_BudgetPractices.pdf

- All project initiatives have a sound Business Case with analysis of benefits, investment costs and long term operational costs

ICT support of budget planning and monitoring

As to the ICT support of the budgeting process, in most countries there is an automated budget management system covering budget planning and monitoring.

E.6.3. GOALS RELATED TO THE AREA

Mid-level ICT goals

- Improved financial planning and cost control
- Distributed responsibility across the sector for operational and investment budgets
- Total cost of ownership is calculated at investment decisions
- On-the-track implementation projects

E.6.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- Experience of ICT staff in operation of judicial systems

Weaknesses

- Statistical ICT system capabilities are underdeveloped
- ICT staff numbers too low, no specialization of ICT roles
- IT operations are fragmented (staff, procurement, maintenance)
- Lack of established performance measurement system for ICT
- Ministry budget is heavily constrained
- Budget planning is constrained by governmental accounting rules, the budget structure is not reflecting all aspects of ICT costs

Opportunities

- EU accession process opens new funds for developments
- Continuing availability of donor funding to finance developments
- ICT Strategy is under preparation to give a framework to and coordinate development efforts
- Governmental e-Government development efforts may provide additional resources

Threats

- Growing maintenance costs as a result of donor-funded ICT developments and purchases
- Growing budgetary pressure and expenditure cuts

E.7. ENSURE HIGH QUALITY USER EXPERIENCE

E.7.1. RELEVANT PARTS OF DIAGNOSIS

In the current situation of the Serbian Justice sector, the main characteristics of end-user environment are the following:

- About half of the workstations is over the age of 6 years
- Windows XP represents about 75% of operating systems run on the workstations
- the proportion of portable equipment (laptops, tablets) is low
- although MS Office is installed on about 74% of workstations, the usage of Open Office is widespread at certain segments of the sector
- Ministry's annual budget covers the renewal of about one sixth of all workstations yearly
- the printers are mainly desktop printers with relatively high maintenance costs and efforts
- scanners are mostly low capacity flatbed scanners without automatic paper feed
- No wireless LANs are used at judicial organisations
- Server rooms are located at each physical locations with the basic conditions for uninterrupted operations (UPSs, air-conditioning, fire-alarm systems) but lack of strong physical security measures (i.e. ID card usage for physical entrance, video surveillance, etc.)

E.7.2. INTERNATIONAL TRENDS AND EU PRACTICE

Some of the trends and practices are the following:

- **Modern technology IT workstations for staff** - The staff of the justice system have the same modern working tools available to them as do employees in the private sector of the economy.
- **Access to applications irrespective of location** - Access to the applications is intended to be possible irrespective of where one's office is located, i.e., all of the applications should be serviceable at all workstations in the justice system, provided that the user has the necessary authorisations. This practice could extend as well to mobile bailiffs, improved flexibility of secretarial deployment, cross-office and disposition of cases and achieving workload balance.

E.7.3. GOALS RELATED TO THE AREA

Mid level ICT goals:

- Availability of proper and trusted information at proper time to authorised people to facilitate decisions
- Standardised and optimised IT operational procedures
- Central management of significant part of IT equipment without the need of physical interaction
- Usage of standardised systems for support functions (HR, budgeting, finance, inventory, etc.)
- Performance of end user environment is supporting everyday tasks

E.7.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- Well developed network infrastructure (WAN and local) at most sites
- Recent efforts to modernize key data centres
- Partly modernized end-user working environment
- Experience of ICT staff in operation of judicial systems

Weaknesses

- Insufficient or inefficient peripherals (scanning capacity, desktop printers)
- ICT equipment partly outdated and should be replaced until the rollout of current case management developments
- ICT staff numbers too low, no specialization of ICT roles
- IT operations are fragmented (staff, procurement, maintenance)
- Ministry budget is heavily constrained

Opportunities

- Continuing availability of donor funding to finance developments
- EU accession process opens new funds for developments
- Price of new technologies and unit price of some capacities (i.e. storage) are decreasing,
- Governmental contract with Microsoft to cover licences for Office products

Threats

- Growing maintenance costs as a result of donor-funded ICT developments and purchases
- Growing budgetary pressure and expenditure cuts
- Talented ICT professionals, well-trained experts / trainers may be drawn away to the private sector with a promise of better salaries and career paths

E.8. ENSURE SUPPORTIVE WORKING ENVIRONMENT

E.8.1. RELEVANT PARTS OF DIAGNOSIS

As mentioned earlier, the Justice sector in Serbia is using a variety of ICT systems covering different organisational entities of the sector and providing different sets of functionalities for these entities. Most of these ICT systems are designed, developed and implemented specifically for certain Justice sector branches, without having in mind if there are comparable or similar requirements in the other branches. For some, either they were planned having uniformity in mind, the past and/or current situation didn't provide possibility for full implementation. As an example, lack of funds has been seen as one of the reasons for not having any ICT system within the Misdemeanour Courts.

All Basic and Higher Courts (including their court units) in Serbia are using Court Case management system named AVP (Automatizovano Vodjenje Procesu). AVP is computerised case event management system that helps judges and court staff through providing online information for monitoring of case progress.

Basic functionalities of AVP are:

- Manage basic information on cases;
- Records of judges responsible for the case and who had previously worked on the case;
- History of all actions and decisions on the subject;
- Records of the interconnections of the case;
- Records of participants in the proceedings with all the data;
- Monitoring of court fees to the level of billing, collection and treatment of all the taxes;
- Scanning of documents in a particular case and creating electronic database of all cases;
- Word templates for all documents created within the court.

AVP is designed and implemented as distributed information system; the application is running locally, within each court. This was a requirement when the system was set up, having in mind unreliable computer network of the courts. This type of architecture is outdated nowadays, particularly that the courts computer network is reliable; the features of interconnectivity of AVP are at the low level and the accuracy of the collected data is not on satisfactory level.

All Commercial Courts are using AVP since 2008. The system fulfils most of the functionalities needed by the commercial courts, having the same characteristics as explained above.

The Misdemeanour Courts are not using any ICT system at the present. However, the project has started in May 2012, in order to automate functions of this type of courts. The project is in early stage, after successful implementation it shall be deployed in all 45 Misdemeanour courts in Serbia.

The Ministry has started a pilot project for implementation of a unified software solution facilitating accurate data collection on efficiency, for both Courts and Judges and providing adequate public access to information pertaining to judicial proceedings and statistics. Implementation of the project is under responsibility of MoJPA and the Supreme Court of Cassation. The software, named SAPS (Standardizovana Aplikacija za Pravosudje Srbije), is currently implemented as Pilot in: **Supreme Court of Cassation** and **Administrative Court** in Belgrade, **all Appellate Courts** (Belgrade, Nis, Novi Sad and Kragujevac) and in Higher and Basic Courts in Sremska Mitrovica. It is up at the last two places from November 2012.

It consists the functionalities of:

- electronic case management;
- reporting and monitoring;
- on-line help;
- generation of predefined documents;
- resources management;
- electronic exchange of information;
- administration;
- document management system.

SAPS is a centrally run and managed software application, for all types of courts. It unifies previous software applications, providing their features and adding the missing ones. The software is designed as modular and developed using readily available software tools. It is based on the enterprise content management (ECM) system to fully support the process of digitalization of paper based work within the Courts. However, the system is not fully rolled out, it is in testing phase. It hasn't jet justified its performances with the bigger courts, as it is only implemented in smaller courts in Sremska Mitrovica.

The **Prosecutor's Offices** don't use any ICT systems today. But, the Software Application for Prosecution offices (SAPO) is under development. As the project started in April, the plan is to implement SAPO in 13 offices in Serbia. It shall consist of various sub systems and modules supporting different functions in the Prosecution Organization. It will provide:

- content management;
- document scanning;
- case management;
- various on-line statistical reports, both internally and externally;

SAPO will cover all business needs and processes within the PO, and provide sufficient capability to link it with other parts of the justice system, the courts and the prison administration systems. In order to ensure easy compatibility and functional integration with the currently developed courts system (SAPS), the solution is based on an enterprise content management (ECM) system, configurable and tailored to the specific requirements of the PO.

The **Administration for execution of Penitentiary Sanctions** - AEPS is currently using several in-house developed central applications fulfilling some of the functionalities needed by the institution. In order to improve the functionalities, AEPS has decided to start a new project, implementation of integrated Software Application for Prison Administration (SAPA), which shall replace all current applications with one integrated solution, implementing all functionalities related to the AEPS activities regarding the prisoners, guards and arms management.

The SAPA could be divided in two main functional integrated sub-systems:

- PDL Personal Records registration (PDL = Persons Deprived of Liberty)
- Prison Functional operations.

The PDL Personal Records refers to the data and information that is related to the PDL personal profiles, activities and the events during the life in prison, while the Prison Functional operations refer to operations where the PDL is interacting with the Prison Operations and/or Services. These interactions between the PDL and the Prison Operations need to be registered, monitored in SAPA to the most details reasonably. In order to ensure easy compatibility and functional integration with the currently developed systems (SAPS and SAPO), the solution is based on an enterprise content management (ECM) system, configurable to the specific requirements of the AEPS.

The **Directorate for Management of Seized and Confiscated Assets** has started in May 2012 a project for two applications, Document and Case Management System and Asset Management System. The software solutions are implemented and are running in DMSCA premises. The Document Management System consists of the next functionalities:

- Manipulation of documents (creation, processing, distribution, storing, indexing and searching);
- Archive;
- Scanning;
- Import and conversion of documents in different formats;
- Workflow management

The Case management software consists of the next functionalities:

- Electronic case dossier;
- Standardized forms;
- Workflow management;
- Management of case resources (staff, rooms, cars);
- Preparation of prosecution file;
- Reporting and Analytics;
- Knowledge management;

The Asset management software consists of the next functionalities:

- Management of documentation (contracts; creation and processing of e-documents, indexing and organizing, workflow, archiving)
- Asset management (administration, registration/de-registration);
- Work order management;
- Financial management;
- Reporting;

At the present, the DMSCA doesn't use ICT systems to the full extent. The Asset management and case management systems are implemented having in mind integration with other systems (SAPS, SAPO).

The Ministry of Justice and Public Administration is currently using an application for process management. Until now, the processes of two departments are implemented (Department for international legal aid in criminal matters and Department for international legal aid in civil matters within the Sector for Normative Affairs and International Cooperation). The application – Serbian LURIS, is based on Electronic Document Management System, and used for international legal aid of the Ministry. Its purpose is to contribute to the processing

of requests for legal aid, keep relevant information about the documents of the two departments, document search, and reporting and generating output documents. Main functions are:

- Registering (including attributes and details) and search of international legal requests;
- Registering of events related to the legal aid requests (including changes of status and dates);
- Reporting;
- Template generation;
- Search through the data (person attributes, cases, etc.);

The solution fulfils most of the needs of the two departments for their everyday work. The Ministry has plans to develop specialised software interfaces for exchange of information with the courts and Prosecutors offices in Serbia.

Aside from this, the two departments are using specialised software tools for help of the employees with visual impairment (OCR software is creating MS Word format of scanned documents, other software is used for reading of this documents).

Except the above mentioned information systems, within the Justice Sector exists a number of applications which fulfils certain functionality of some entity, but these are smaller, monolithic applications which are used especially of their own. Such applications are:

- Register of cases in High Misdemeanour Court – electronic evidence of cases;
- Archive in High Misdemeanour Court – electronic archive of cases;
- Training register in Judicial Academy - Register of mentors and candidates for basic training, training through semesters, working hours of mentors, register of lecturers, register of certificates issued;
- Budget application in the High Council of Courts and the Ministry;
- HR application in several courts;
- Book of post in several courts;
- Archive in several courts;
- Register of compliances and appeals in several courts;
- Register of requests in several courts;
- Electronic evidence of laws, regulations, court practice, forms in several courts;

As well, there is a centralised portal for courts (www.portal.sud.rs) which is described in Section 6.1.

E.8.2. INTERNATIONAL TRENDS AND EU PRACTICE

International trends regarding the functionalities of the Justice sector information systems vary within different countries based on the legislation and the scope of activity. But, there is an approach common for almost all countries, the moving toward common IT architecture and introduction of flexible, loosely coupled components which could be easily interconnected, together with development of sets of data exchange standards. For example, Austria has introduced Service Oriented Architecture in order to standardize its information systems and enable for reuse of different IT components with same or similar functionalities for different Justice sector entities. Another common approach is use of single registers for all organisations, which is eliminating the possibility of use inaccurate data. Such examples are present in Austria, Netherlands, and Estonia. Moreover, there are EU joint projects toward interconnection of common registers and exchange of information between EU members, as Land register, Business register and others. E-CODEX is another joint project of 14 EU members, aiming to improve the cross-border access of citizens and businesses to legal means in Europe as well as to improve the interoperability between legal authorities within the EU. It aims to build a pan-European interoperability layer by connecting the existing systems that will allow communication and data exchange based on the development of common technical standards and foster cross-country cooperation in the area of European e-Justice. As well, there are example of ICT systems which provide advanced services and functionalities. For example, in Turkey is running SMS judicial information system which provides an outstanding service for the citi-

zens and lawyers which enables them to receive SMS messages containing legal information such as on-going cases, dates of court hearings, the last change in the case and suits or debt claims against them.

European Union has adopted a European e-Justice strategy in 2008. Within the strategy, it prescribes the European Justice Portal a one-stop-shop for citizen's access to any legal means. Some simpler procedures are automated and accessed from anywhere within the EU, as order for payment, small claims, online payment of procedural costs, legal aid, registers of translators and interpreters, videoconferencing, alternative dispute resolution, etc.

E.8.3. GOALS RELATED TO THE AREA

Mid-level ICT goals:

- Availability of proper and trusted information at proper time to authorised people to facilitate decisions
- Availability of proper information for the participants of particular judicial processes
- Usage of standardised systems for support functions (HR, budgeting, finance, inventory, etc.)
- During implementation of ICT system parallel development of the same functionality is eliminated
- The Role of manual information exchange processes is reduced within the sector and with other actors
- All judicial institutions are using the same master data
- Having a standardised application environment
- Institutional processes are coordinated whenever new ICT systems are implemented / modified

E.8.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- State of the art Case Management systems at some institutions
- New Case Management systems are developed on same platform
- Recent efforts to modernize key data centres
- Several mid-range servers will be available for other duties after SAPS implementation
- Existing coordination of ICT development efforts
- Well established organisational responsibilities to finance and manage donor projects

Weaknesses

- No practice of the use of electronic signatures
- Insufficient or inefficient peripherals (scanning capacity, desktop printers)
- Fragmented case management systems, 3 separate ongoing implementations (SAPS, SAPO, SAPA)
- ICT equipment partly outdated and should be replaced until the rollout of current case management developments
- Communication bandwidth is not wide enough at certain locations
- End user affinity to usage of ICT tools is varying from low to high
- Ministry budget is heavily constrained

Opportunities

- EU accession process opens new funds for developments
- Continuing availability of donor funding to finance developments
- Price of new technologies and unit price of some capacities (i.e. storage) are decreasing

Threats

- Perpetual changes in the institutional framework of the justice sector
- Reluctance of other governmental agencies to establish electronic data channels

E.9. ENSURE HIGH AVAILABILITY AND RELIABILITY

E.9.1. RELEVANT PARTS OF DIAGNOSIS

The Justice Sector IT environment is built up having in mind the basic fault tolerance (or high availability) features. Following the problems faced in practice, the Justice Sector has applied some redundant components in different parts of the system:

- disk mirroring and data backup;
- set up of fault tolerant network infrastructure;
- set up of parts of the IT infrastructure virtualized;

The Justice Sector has planned the disaster recovery centre, but the project has still not started.

E.9.2. INTERNATIONAL TRENDS AND EU PRACTICE

In the today's usage of ICT within the almost every part of our lives, there is a big pressure over the business, and as well, the public sector to ensure supportive working environment and high system availability for its clients. The same principle is applicable for the justice sector. Some of the trends and practices are the following:

- **High availability of business-critical applications** - Business-critical IT solutions are defined as such, and are developed to respond to the special requirements of the justice system. Within the defined core periods, they are operated as highly available and highly performing IT-systems.
- **Security of IT solutions** - The goal of IT security is to ensure availability of IT solutions (including the data), to assure the authenticity, integrity and confidentiality of the data and to prevent use of or damage to the IT solutions by unauthorised persons. IT security is intended to cover all of the facilities (both systems and individuals) which are at risk and which require protection. These include inter alia buildings, hardware and software, networks, communications systems, operating instructions and other software solution documentation, the users of the IT systems and support facilities such as the help-desk.
- **Provision of management information** - An organisation's ability to perform optimally will also depend on the availability of meaningful performance data. These will form the basis e.g. for documenting the processes of judicature, management decisions on controlling the organisation of the justice system, supporting the legislative branch, monitoring the length of proceedings, monitoring prison capacity and implementing prison system planning, optimising staff deployment and documenting overtime, controlling, etc.
- **Successful methods for developing and operating IT solutions** - In order to ensure the greatest possible efficiencies of legal informatics, modern models and methods of software engineering and work organisation are used for developing and operating the IT solutions.
- **Cloud computing** solutions not only provide a more cost efficient solution to provide computing power, but may contribute to increased reliability of services if proper virtualisation solutions are used.

E.9.3. GOALS RELATED TO THE AREA

Mid level ICT goals:

- Availability of proper and trusted information at proper time to authorised people to facilitate decisions
- High availability of judicial IT systems
- Standardised and optimised IT operational procedures
- Central management of significant part of IT equipment without the need of physical interaction
- Requests towards IT are registered and tracked by uniform IT application
- Usage of standardised systems for support functions (HR, budgeting, finance, inventory, etc.)
- Performance of end user environment is supporting everyday tasks

E.9.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- Well developed network infrastructure (WAN and local) at most sites
- Recent efforts to modernize key data centres
- Partly modernized end-user working environment
- State of the art Case Management systems at some institutions
- Experience of ICT staff in operation of judicial systems

Weaknesses

- Insufficient or inefficient peripherals (scanning capacity, desktop printers)
- No separate ICT infrastructure and ICT staff for prosecution offices
- ICT equipment partly outdated and should be replaced until the rollout of current case management developments
- Communication bandwidth is not wide enough at certain locations
- ICT staff numbers too low, no specialization of ICT roles
- IT operations are fragmented (staff, procurement, maintenance)
- Ministry budget is heavily constrained

Opportunities

- Continuing availability of donor funding to finance developments
- EU accession process opens new funds for developments
- Price of new technologies and unit price of some capacities (i.e. storage) are decreasing,
- Governmental contract with Microsoft to cover licences for Office products

Threats

- Growing maintenance costs as a result of donor-funded ICT developments and purchases
- Growing budgetary pressure and expenditure cuts
- Talented ICT professionals, well-trained experts / trainers may be drawn away to the private sector with a promise of better salaries and career paths

E.10. ENSURE HIGH EFFICIENCY

E.10.1. RELEVANT PARTS OF DIAGNOSIS

The establishment of centralized unit for ICT in Justice Sector aims at higher efficiency in terms of ICT staff utilisation. In technical terms one of the major contributors to efficiency in the internal unification and standardization of procedures and technical solutions.

The key findings of the diagnosis are the following:

- The currently used various Case Management systems are not utilizing electronic communication channels, but a unification process has been started.
- Although there is a centralized portal for courts, this has not fully built-in transactional possibilities, but instead it serves as an entry point to the different court portals often having different structure and differing Common Look and Feel (CLF) standards.
- Local ICT related procedures are not based on centrally-issued and controlled policies, but developed locally.
- Major development projects are managed usually according to methodology of the various vendors and apart from cost/budget control there is no uniform project management methodology within the Justice Sector.
- Application environment at the end-users is heterogeneous, even document exchange is sometimes cumbersome because of different document formats (MS Word 2003, 2007, Open Office)
- Although there are commonly used software for certain activities (i.e. accounting), there are a lot of locally developed applications for the same or very similar functions (e.g. case law, registry books, etc.)
- Reports on the work and performance of various institutions ("*Informator o radu*") have no uniform structure and content

E.10.2. INTERNATIONAL TRENDS AND EU PRACTICE

Many judicial organizations take advantage of the potential opportunities offered by the unstoppable development of information technologies. The use of ICT for the delivery of public services (e-Government services) requires a very high level of security to ensure its availability, integrity and confidentiality on a permanent basis.

The international trends in unification of IT services are mainly focused on the ensuring the proper level of data security and citizen's privacy in a context of evolution of information technologies. The judicial organizations should make appropriate strategic and tactical choices in order to reduce the risks. Such choices should be related not only to the devices, machines and technology, but also to the human, legal, regulatory and governance issues.

European Network and Information Security Agency

At the end of 2012 and thus the beginning of 2013 the European Network and Information Security Agency (ENISA - <http://www.enisa.europa.eu/>) published 'Final report on Risk Mitigation Strategies and Good Practices' http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/COIT_Mitigation_Strategies_Final_Report/at_download/fullReport and 'Critical Information Infrastructure Protection perspective on cloud computing services' http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing/at_download/fullReport, which present security policies that can be deployed to mitigate risks.

Council of European Union

Article 10 – ‘Protection of EU classified Information handled in communication and information systems’ of Council decision of 31 March 2011 on the security rules for protecting EU classified information (2011/292/EU) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:141:0017:0065:EN:PDF> defines the Information assurance concept, which is obligatory for communication and information systems handling EU classified Information, including Case Management system managed by the European Union's Judicial Cooperation Unit – EUROJUST.

E.10.3. GOALS RELATED TO THE AREA

Mid level ICT goals:

- Unified project management procedures and central unit responsible for sector-wide IT projects
- Availability of Information Exchange Standards (between the judicial institutions, and cross-governmental exchange)
- Availability of Registry of Software Licences to ensure compliance and utilisation planning
- ICT development, project management and operation procedures are based on the same standards across the justice system
- All judicial institutions are using the same master data
- Usage of standardised systems for supporting functions (HR, budgeting, finance, inventory, etc.)
- Having a standardised application environment
- The role of manual information exchange processes is reduced within the sector and with other actors, in favour of standard-based electronic data/information exchange
- On-track implementation projects

E.10.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- Partly modernized end-user working environment
- New Case Management systems are developed on same platform
- Existing coordination of ICT development efforts
- Well established organisational responsibilities to finance and manage donor projects

Weaknesses

- Fragmented case management systems, 3 separate ongoing implementations (SAPS, SAPO, SAPA). Either the 3 systems provide interoperability features, there are common functionalities which are not considered when planning and designing the systems.
- No information sharing standards defined on the semantic level
- Lack of established performance measurement system for ICT
- Lack of formalised methods/forums to inform (or request comments from) HJC and SPC on ITC related decisions

Opportunities

- EU accession process opens new funds for developments
- ICT Strategy is under preparation to give a framework to and coordinate development efforts
- Governmental contract with Microsoft to cover licences for Office products
- Availability of international standards for regulation of various aspects of ICT developments and operations

Threats

- Lower level regulatory items are missing (i.e. bylaws for Digital Signature) or are created very slowly

E.11. ENSURE INFORMATION SECURITY

E.11.1. RELEVANT PARTS OF DIAGNOSIS

The diagnosis 0073 related to the ICT systems sustainability is mainly in the “Technology architecture” and “ICT Process Maturity assessment” sections of the Diagnostic Report. The key findings are the following:

- There is no formal methodology used to assess and manage risks. Major risks are recognised intuitively (maturity level of “PO9 Assess and Manage IT Risks” process area is currently 1)
- Daily backups are prepared but off-site storage is not solved for backups. Disaster Recovery Plans and Business Continuity Plans do not exist. (maturity level of “DS4 Ensure Continuous Service” process area is currently 2)
- There is a specialised group within Ministry (Supervision of the Secrecy of Data) which demonstrates high importance, and most important security controls, like user authentication/authorisation are in place (maturity level of “DS5 Ensure System Security” process area is currently 2)
- Physical environment of larger institutions possess of basic security controls (i.e. dedicated space for servers, air conditioning), but smaller institutions may face challenges (maturity level of “DS12 Manage the Physical Environment” process area is currently 2)
- Even established control mechanisms are sometimes hard to evaluate. For example AVP transactional logs are analysed only after suspicion of security breaches. (maturity level of “ME2 Monitor and Evaluate Internal Control” process area is currently 2)
- For some IT resources there are redundancies (i.e. for WAN network, certain servers)
- Backup sites are being built
- Basic elements of security architecture are implemented (i.e. virus scanners, firewalls)
- Procedural level security directives are not formulated and not controlled.

E.11.2. INTERNATIONAL TRENDS AND EU PRACTICE

In most European (and other) countries IT security is a distinguished factor of IT operations and IT strategies since one of the major objectives is to maintain transparent, reliable and secure judicial processes. Some IT strategies (i.e. Turkey, Macedonia, Bulgaria) prepared during the recent years explicitly contain references to IT security related tasks.

IT Security is a well established segment of the overall IT with several standardisation efforts during the last two decades. Major emerging frameworks are

- CoBIT for IT governance,
- ISO 27000# family (based on formal British Standard 7799) for IT security management and
- Common Criteria for computer systems security specification.

These frameworks/standards slightly overlap and have are using different approaches. While CoBIT originates from an audit methodology, ISO 2700# family is a full standard for all aspects of security procedures and management. Therefore this is maybe the most widespread standard used or planned to be used in current European justice organisations.

Implementation of an ISO 27000# compliant security system is among the goals of several governments related to the increased role of e-Government applications (both Government to Consumer and Government to

Government developments). Thus the drivers to implement ISO 27000# compliant system is often derived from overall governmental objectives but the implementation can be done in isolation of the Justice Sector as well.

Even if a full implementation and certification standards of ISO 27001# is not declared, some crucial elements of the standard are followed in the strategies:

- There is a common understanding that an overall IT Security Policy is needed for the Justice Sector
- IT security related trainings of IT staff and the end-users is regarded as a critical factor
- Some key technical elements (like digital signatures, restriction of physical access of IT equipment, etc.) are commonly aimed at.

On overall European Union level there is no required single standard, but the general practice is to put heavy emphasis on the issue and to rely on international standards.

E.11.3. GOALS RELATED TO THE AREA

Mid level ICT goals:

- Improved security of access to the information and data - Identity management and data protection
- Availability of registry of Software Licences to ensure compliance and utilisation planning

E.11.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- Basic security measures have been taken (anti-virus, spam filtering)
- Recent efforts to modernize key data centres
- Experience of ICT staff in operation of judicial systems
- ICT staff members have knowledge of international security standards (ISO 27000)

Weaknesses

- No practice of the use of electronic signatures
- Insufficient security measures (logging) and awareness, attitude and knowledge about data security issues
- ICT staff numbers too low, no specialization of ICT roles
- End user affinity to usage of ICT tools is varying from low to high
- Ministry budget is heavily constrained

Opportunities

- New legal regulations affecting electronic state administrations (i.e. planned law on data security)
- EU accession process opens new funds for developments
- Availability of international and national standards for regulation of various aspects of ICT developments and information security

Threats

- Growing budgetary pressure and expenditure cuts
- Lower level regulatory items are missing (i.e. bylaws for Digital Signature) or are created very slowly

E.12. INCREASE KNOWLEDGE AND PROFICIENCY

E.12.1. RELEVANT PARTS OF DIAGNOSIS

Some key findings related to the role of the Judicial Academy and the ICT trainings:

- Judicial Academy was established in 2002, significant changes about the name and functionality took place in 2010.
- There is an existing plan to make changes in structure, job classifications and job descriptions of the Judicial Academy in the near future.
- In the sector the following most common trainings are organised:
 - Initial judicial training for all newly elected judges and prosecutors;
 - Continuous judicial training (seminars) for the judges and prosecutors;
 - Trainings for end-users of freshly implemented ICT systems provided by the vendors
 - Sporadic basic ICT trainings for end-users
 - Specialised ICT related trainings for ICT staff

The first two training types are to be supported by ICT tools; the next three training types have ICT as the domain/area.

Trainers: for the judicial topics mostly judges and prosecutors, teachers/lecturers from the universities are involved too. The Ministry of Justice and Public Administration organises training events about ICT topics: training sessions together with the suppliers' and separate seminars, to support local ICT staff and end users.

In addition to formal ICT trainings, ICT staff of the institutions is acting as coaches, to support every-day work of employees which needs ICT skills.

Annual Training plan exists with around 150-200 training seminars organised per year (incl. regions).

As to the training ICT infrastructure, Judicial Academy possesses mainly modern workstations/laptops and an internal LAN satisfying the needs. In-house developed application "Basic/permanent training" is implemented to register mentors/candidates for basic training, semesters, lecturers and issued certificates. Judicial Academy also established Video conferencing equipment together with the 4 Appellate Courts, but the currently very low bandwidth of their Internet connection prevents the usage.

Other plans and strategies: within the EuropeAid project "System for the monitoring and evaluation Judicial Academy" (2010), the Plan of Implementation was developed as well, to support the Judicial Academy and improve training. One of the priorities, related to ICT, was: "Strengthening the institutional capacity of the Judicial Academy to organize training and evaluation of training with the introduction of appropriate IT systems" was not settled yet.

Knowledge sharing of judicial cases

Practically all courts have their own case law departments whose major task is to analyse and publish decisions which might be utilised in similar cases. Publication (if any) is done on the web pages of the individual courts and currently there is no central register for all interesting cases. Naturally the higher instance courts has more significant role in this process than lower instance courts. The publication scheme is following the system of "registers" and is not searchable. In theory the implementation of the centrally operated SAPS system may enable users to access all relevant information on cases.

However the publication of the cases is covering only a small part of all cases at a given court, majority of results of the case law departments is stored on internal file systems or Intranets.

The most widespread tools to access closed cases are the systems provided by the commercial legal databases: ParagraphLex, Intermex Court Practice and Propisi.net.

Knowledge sharing (publication) has other forms: some articles are published in paper based form and the trainings at the Judicial Academy also devote significant amount of time to case law.

Knowledge sharing within functional departments

Functional departments derive their tasks from "Court Rulebook" which in turn is derivative of laws and higher level regulations. Although there can be slight differences in operations and applied methods, but there are no established forums for exchanging ideas and best practices.

Knowledge sharing between IT units

As the Diagnosis Report demonstrated, the IT units of the justice system are fragmented. There is cooperation between the various courts located in the same building wherever this is the case, but cooperation and knowledge sharing between IT personnel in different cities practically does not exist, even if the IT staff operates the same systems and faces the same challenges.

For some local requests local responses are given, several small scale applications are developed by local IT staff without sharing their practice. There is no mechanism to exchange ideas and roll-out locally developed tools.

E.12.2. INTERNATIONAL TRENDS AND EU PRACTICE

According to data, obtained through public websites via different portals, the training of Justice sector is centralised in most of the countries – usually, there is one legal body/institution, responsible for the education and training of the whole Justice Sector of the country.

The legal form and names are very different, it can be public, non-profit/non-governmental institution (e.g. Canada, Bulgaria), foundation (e.g. Latvia), national institute (e.g. Romania), public institution that has its own patrimony, self-management, scientific and pedagogical (Moldova), self-governing body (Italy), an affiliated body of the Ministry of Justice (e.g. Slovenia, Finland), part of the National Courts Administration (Sweden) or department of the Supreme Court (Estonia).

Types of activities of the centralized training institution (in most of the countries):

- Recruitment, education and training for judicial staff: initial and continuous training
- Training for non-judicial staff
- Organization of competitions and examinations
- Training of trainers (e.g. Canada: principles and processes of course design for judicial educators and court education committees)
- analysing and identifying training needs, as well as designing programmes and methods for judicial training (e.g. Italy)
- ICT skills training (e.g. Canada, Estonia)
- Distance-learning courses (e.g. Bulgaria)
- Publishing activities: publication and distribution of juridical publications (e.g. Latvia), training materials via website (e.g. Moldova, Bulgaria), virtual Library on website (e.g. Moldova)
- Maintaining the institution's website
- Coordination of international cooperation of judges and other activities (e.g. Latvia, Bulgaria, Slovenia)

- Organization of international seminar and conferences (e.g. Latvia)
- Logistical support court-based program delivery in venues throughout the country (e.g. Canada)
- Carry out the activities of a Documentation Center in EU Law for the Judiciary (e.g. Bulgaria)

The training events are mostly lectures, but also seminars, roundtables and other types of trainings may be used.

For basic ICT trainings most countries around the World support the acquisition of European Computer Driving Licence (ECDL) and in some cases ECDL (or a demonstrated IT knowledge of this basic level) is de facto prerequisite to fill a job. In case of some EU countries (e.g. Ireland), ECDL acquisition for justice professionals is significantly supported and formulated as part of the ICT strategy. Although it is well beyond the scope of our project, but nevertheless every governmental level initiative of spreading ECDL within the public administration might help the Justice Sector as well.

Information sources:

- The International Organization for Judicial Training (IOJT), promoting the rule of law by supporting the work of judicial education institutions around the world: <http://iojt.org/iojt2/page201membersa.html>
- The European Judicial Training Network (EJTN): <http://www.ejtn.net/About/About-EJTN/> is the principal platform and promoter for the training and exchange of knowledge of the European judiciary. EJTN represents the interests of over 160,000 European judges, prosecutors and judicial trainers across Europe. EJTN's fields of interest include EU, civil, criminal and commercial law and linguistics and societal issues training. The vision of EJTN is to help to foster a common legal and judicial European culture. EJTN develops training standards and curricula, coordinates judicial training exchanges and programmes, disseminates training expertise and promotes cooperation between EU judicial training institutions.

Knowledge sharing (or using the terminology of business environments: knowledge management) became one of the major development areas of organisations relying heavily on human capital and knowledge of individual employees. Sharing ideas, best practices and lessons learnt is not only saving resources for the organisations, but contributes to the overall quality and what is sometime even more important: quicker procedures.

Justice Sector with its fragmented and geographically diverse organisation is a key application area of knowledge sharing, therefore jurisprudence is present in the legal system of virtually every countries.

EU level

On European level the European Network of Councils for the Judiciary promotes case law developments. On EU level, the current situation is far from being complete, it mainly focuses on enforcing the European level regulations to the local judiciary systems of the member states by the European Court of Justice. Also on EU level the EUR-LEX database provides a searchable interface to all European Court Cases.

Currently an European Case Law Identifier (ECLI) is being introduced in member states but without obligatory deadlines for the member states⁵. According to an EU Council Conclusion from 2011, candidate countries are encouraged to use the ECLI system⁶. ECLI only a structured identifier with a defined minimal metadata set.

⁵ Source: https://e-justice.europa.eu/content_european_case_law_identifier_ecli-175-EU-en.do?clang=en

⁶ Source: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:127:0001:0007:EN:PDF>

National levels

Implementation of ECLI is not obligatory for member states, but some countries has already built this identifiers to their systems and some others are implementing it.

On national levels however case law database has large significance. One of the best examples is the Judicial Documentation Centre of Spain which was established in 1996. Through a searchable database it provides open access to everyone to all decisions of the Spanish legal institutions. The upload latency time is very short; the freshest published decisions are only 2 weeks old⁷.

Similar centres already exist in the region for example in Bosnia and Albania.

E.12.3. GOALS RELATED TO THE AREA

Mid-level ICT goals

- IT operations staff possess the required ICT knowledge
- Decision makers are aware of the role and importance of ICT
- Legal professionals and court administration is knowledgeable on effective use of ICT
- Well defined and organised training process (plan-organise-coordinate-evaluate) made efficient by using ICT tools
- e-learning tools are in place to facilitate mass trainings
- End-users and staff members with deep knowledge on procedures are involved in IT developments
- Knowledge and practices are shared, easy to find, uniformly interpreted and constantly applied

E.12.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- State of the art Case Management systems at some institutions
- New Case Management systems are developed on same platform
- Well-equipped training facilities in four different regions;
- Enthusiastic and competent training and IT staff in the Judicial Academy.

Weaknesses

- Electronic archiving is not implemented
- Fragmented case management systems, 3 separate ongoing implementations (SAPS, SAPO, SAPA)
- No information sharing standards defined on the semantic level
- IT operations are fragmented (staff, procurement, maintenance)
- No systematic approach for establishing training needs, including ICT training needs;
- No modern ICT tools to support the whole training process (planning, organising, coordination, evaluation, statistics etc.);
- Insufficient coordination of ICT training, insufficient cooperation between Ministry and Judicial Academy;
- No existing electronic database of experts/ trainers/ possible trainers of different areas;
- Existing website of the Judicial Academy is static, not updated and interactive enough;
- No electronic tools/ databases for the publication and distribution of training materials (eg. court cases, manuals);

⁷ See search interface at: <http://www.poderjudicial.es/search/indexAN.jsp>

- Insufficient training staff in the Judicial Academy
- Low bandwidth Internet link. at the Judicial Academy prevents parallel video-conferencing even with the established video-conferencing sites

Opportunities

- Knowledgeable business partners having accumulated deep knowledge of the justice ICT
- Price of new technologies and unit price of some capacities (i.e. storage) are decreasing,
- Vision of restructuring the Judicial Academy exists (incl. establishing of the separate IT unit);
- Implementation Plan of the System for Monitoring and Evaluation of the Judicial Academy exists;
- Continuing cooperation with the NGO's and businesses, aiming to organise common training events.

Threats

- Perpetual changes in the institutional framework of the Justice Sector
- Well-trained experts / trainers may be drawn away to the private sector with a promise of better salaries and career paths.

E.13. ENSURE WIDELY AVAILABLE WEB-BASED SERVICES FOR ALL USERS

E.13.1. RELEVANT PARTS OF DIAGNOSIS

Ministry

By its nature, Ministry web-page is primarily providing information on the whole legal environment and operations of the whole sector with no transactional services.

Courts

The majority of direct interactions between the citizens and the Justice Sector are during the various court procedures, thus this area has primary importance in developing e-Services.

Access to Internet services of the judiciary in Serbia is possible through web portal at www.portal.sud.rs, through individual portals of each Court and centralized portal for providing services to all public administration. This centralised portal provides general information on the Court System and various queries (mainly related to Commercial Court activities). The interactivity of the portal is limited; its role is mainly information provision.

The portal is not even filled with all data; currently the individual cases and statistics of Commercial Courts can be accessed.

In addition to this central portal, the individual courts all have their own web-portals. Although there are some uniformity effort in design and functions, but they vary from court to court. Some court portals provide only general static information on their operations and some others achieved higher level interaction (e.g. First Basic Court of Belgrade).

Basic, Higher, Commercial and Commercial Court of Appeals have unique information system for case management that in theory enables the display of the procedures into the portal, but in general this feature is not exploited. It is possible to search for data by multiple criteria such as court name, client name, date of receipt of the case, judge name etc. Searching the database provides information on the progress of the case and to the participants in the proceedings, the name of the judge, submitted in writing and other metadata. System

performances are very good in most of cases, but certain slowdown is possible in the biggest courts like First Basic Court in Belgrade or Commercial Court in Belgrade.

Trial schedule allows search of trial terms on several criteria such as the name of the court, term date, name of the judge or case number. The time and date are given by the search, so as the type and status of the term.

In addition to individual case related data, court statistics are available only for some courts. Statistics shows the number of court cases received/resolved for a particular year. Data are presented cumulatively for the court and there is no access to the work of any particular judge. As a general rule, the quarterly and yearly "*Informator o Radu*" documents are also published.

Among the other services on the portal, judicial institutions a list of laws and regulations in the field of internationally significant legal aid stands out. This section of portal also contains checking of court jurisdiction by zip code and name of the city.

The usual information that can be found on web pages are information on the organization of the court, the annual working time schedule, tariffs, taxes and an electronic bulletin board. This last is the fulfilment of all obligations of the court of all public auction published in the bulletin board in the court and on the bulletin board on the Internet. Text ads are located on the accompanying PDF document. Some of the courts within their presentations have a service for ordering documents via mail. Ordering is done by filling out electronic forms until the charging is done via bank transfer to the account of the court. A smaller number of portals provide examples of completed forms and instructions for the preparation of submissions to the court.

A large number of courts have special Web presentation that graphically similar to the solution made for the Supreme Court. Case flow interface could be displayed in Latin and Cyrillic script and in the same manner are showed the search results. Apart from some courts (i.e. First Basic Court in Belgrade) which have some information in English, there is no support for other languages. Accessibility features for seeing impaired people are rarely present.

Prosecutors

Prosecutorial operations are require much less interactions with citizens than court procedures, consequently the presence of this branch of Justice Sector on the Internet is marginal. There is no central portal for the whole prosecutorial organisation, and not all prosecutor's offices have their own web-pages.

The prosecutorial web pages are mainly providing information on the general operations of the branch with no interactivity present.

High Judicial Council

High Judicial Council has its own webpage, containing information on its legal environment, operations and public decisions of the Council, but has no transactional abilities.

State Prosecutorial Council

Similarly, the State Prosecutors' Council has limited functionality on its webpage, its main role is the information provision on legal environment, some aspects of internal operations and the decisions of the Council.

Judicial Academy

Judicial Academy has its own webpage mainly containing information on the operations of the organisation, and there are downloadable documents for certain trainings. Course information is on the webpage, grouped ac-

ording to subject areas, but it is not updated regularly. Because of the large number of interactions between justice professionals and the Academy, the development of the portal can be a major step forward.

E.13.2. INTERNATIONAL TRENDS AND EU PRACTICE

Development of web services in European countries is at different levels of maturity. By rule, court informational systems have highest level of web services being in need for constant communication with parties and administering a job of public interest. We can take justice in Austria as an example of very high level developed system, where especially interesting is system called Electronic legal communication. This system of communication was presented at the beginning of the 1990's but possibility of full electronic communication was introduced by the end of last century. Achievements of this system are significant time, money and labour saving and thus Austrian justice system is often referred to as world leader in IT justice area. Established system and infrastructure lead to advent of large number of software developers who, on the other hand, contributed to the quality of service. General public information is provided on one place, where citizens can, beside insight in general justice organisation, get to know Ministry organisation, read news or subscribe to newsletter.

Justices of Republic of Slovenia and Croatia are especially interesting because of their common justice history. With these two, Serbia shares obligation of adjusting to European standards. Justice system of Republic of Slovenia made significant improvement in department of IT justice. Main characteristics are existence of unique portal for justice which provides insight in work of each court separately or all courts in general. There is connection to CMS of each court so insight of hearing schedules is provided. Portal itself has significant content customization capability for every user and also links to other important elements of justice system. Other justice institutions have portals on their own with mostly general information about institution type, employees and news.

Unlike Slovenia, Croatia IT Justice Sector is at the beginning of development. It is clear that the development roadmap is in introduction CMS to courts which will lead to availability of necessary data to public through web portals.

In widest terms, the provision of web based services for users (and especially for general public) is in line with the ISO 26000 standard (appropriate Serbian standard is SRPS ISO 26000:2011) of "Guidance on Social Responsibility". This standard covers diverse fields from Human Rights and Labour Practices to Community Involvement and Development. This special standard is a guideline which cannot be used for certification or for audits, yet it has recommendations about the above aspects. From ICT perspective, the "Technology development and access" of the Core subject: "Community Involvement..." is the most relevant. Web accessibility is described in detailed in the "Web Content Accessibility Guidelines (WCAG) 2.0"⁸.

E.13.3. GOALS RELATED TO THE AREA

Mid level ICT goals:

- Availability of proper information for the participants of particular judicial processes
- e-Services to the citizens related to judicial proceedings
- Availability of general information on legal system, case-law and performance measures for the public

⁸ Source: <http://www.w3.org/TR/WCAG20/>

E.13.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- State of the art Case Management systems at some institutions
- New Case Management systems are developed on same platform

Weaknesses

- Statistical ICT system capabilities are underdeveloped
- Communication bandwidth is not wide enough at certain locations
- Case management systems are not integrated with existing portals
- Transactional capabilities of institutional web portals are limited

Opportunities

- Governmental e-Government development efforts may provide additional resources
- Increased requests for e-Services from the public, from legal entities, from attorneys, from public notaries and private enforcers
- Create institutional identity through unified vision of all judicial bodies

Threats

- Perpetual changes in the institutional framework of the Justice Sector

E.14. MAINTAIN VARIOUS DELIVERY CHANNELS AND STIMULATE USAGE OF MODERN ICT RESOURCES

E.14.1. RELEVANT PARTS OF DIAGNOSIS

The exchange of information in the Serbian Justice Sector today is still very much in the “traditional”, old-fashioned way; there are numerous couriers, carrying physically heaps of paper documents between various Justice Sector institutions, as well as to and from other governmental institutions, public companies, etc. (excluding one exception of judicial portal, as explained later). The delivery of the courts’ documents to participants in a case, lawyers, court experts, and others involved in court cases goes mostly through snail-mail, ensuring that the whole process is painfully slow and inefficient. It is safe to say that this is one of the most significant reasons for courts inefficiency, length of cases, delay in resolving cases, etc.

Although laws on electronic signature and use of electronic documents were passed in the parliament several years ago, their use in real life, including judiciary, is not progressing at any reasonable rate, and these methods of communication are still considered, by and large, as unsafe, almost dangerous; the reasons for this attitude stem mostly from no real change management and communication campaign by the authorities, i.e. no well-thought effort to publicize and explain clearly the advantages of these new ways of doing business, not just in the Justice Sector, but in many other areas of business and/or public life.

However, one must notice also some improvements in the last several years, mostly reflected through the existence of the “Judicial portal”, used to provide essential information on most of the cases sitting at either commercial or general-jurisdiction courts across the country. This is de facto the only other ‘parallel” delivery channel for selected information to the general public, delivering at least the essential information on all current cases at most of the courts. This ability is using the new Case Management Systems, both in commercial and common jurisdiction courts, to publish key information on all their cases on a common judicial portal (<http://www.portal.sud.rs/code/navigate.aspx?id=601>), and allow for various searches, using court, judge,

case number or their starting dates as the search parameters. Inasmuch as this kind of information delivery is useful and a huge step towards courts accessibility, it is still lacking the ability to use a “push” technology to deliver key case and other judicial information to an individual client, depending on his/her needs.

E.14.2. INTERNATIONAL TRENDS AND EU PRACTICE

The European Union (EU) is acting to facilitate cross-border cooperation between courts and among legal practitioners. Legislative instruments have been introduced to help speed up cross-border proceedings, to take account of other Member States' criminal judgments and to use information technology to make the legal systems of the Member States more accessible to the general public and to legal practitioners.

In December 2009 the European Union Member States adopted a new multiannual programme – the “*Stockholm Programme*” – setting out priorities for the next five years with a view to the creation of an area of freedom, security and justice across Europe (as published on European e-Justice portal). In it, among other goals, it is stated:

- “Work should continue on improving the electronic tools that have so far been developed and the necessary resources should be provided for pursuing this work.”
- “The European Council considers that e-Justice presents an excellent opportunity to provide easier access to justice.”
- The European Council considers that e-Justice presents an excellent opportunity to provide easier access to justice.
- “The European Council invites the Council, the Commission and the Member States to:
 - create effective conditions to enable the parties to communicate with courts by electronic means in the context of legal proceedings;
 - devote efforts to the full implementation of the e-Justice action plan;
 - examine the possibility of dispensing with the formalities for the legalisation of documents between Member States, and submit a proposal to that effect.”

There is ample evidence of efforts across EU countries to enhance their justice systems services to clients and stakeholders through various Customer Service Strategies and other similar approaches, with understanding that each customer, i.e. user of justice services, requires access to information and services that meet their needs. As a result, there is a tendency to modernize service delivery channels and streamline business processes. Obviously, ICT appears as a key facilitator in achieving these goals; some of the key examples of ICT trends include:

- CCTV Links and Video Conferencing Technology
- Digital Audio Recording of court hearings
- Electronic Presentation of Evidence (complex court cases with huge documentary evidence)
- Telephone Interpreting Services (where court clients do not speak native language)

In those countries where the state ability to finance these efforts is insufficient, public-private partnerships (PPP) to deliver equal access for all to the justice system are investigated. The private sector (business and non-governmental organisations) can provide finance, technology and technical skills that are often in short supply in state institutions. Their involvement can also increase public trust.

E.14.3. GOALS RELATED TO THE AREA

Mid-level ICT goals

- Judicial staff can access information independently on the physical location of staff
- e-Services to the citizens related to judicial proceedings
- Availability of proper information for the participants of particular judicial processes
- Usage of multiple communication channels with the public in judicial processes

E.14.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- State of the art Case Management systems at some institutions
- Ability to adjust the delivery to each type of client, satisfying the conditions dictated by the key pillars of the Justice Reform principles
- Ability to manage and influence the popularity and cost of use for each delivery channel, thus improving overall cost-performance goals

Weaknesses

- No practice of the use of electronic signatures
- Document exchange with counterparts is paper based
- No other communication channels except for web portal exist or planned
- Overcoming already-existing public resistance to the use of modern ICT methods of information exchange
- Internal resistance to introduction of modern delivery channels, due to lack of knowledge/education
- Inability to other stakeholders/partners to accept modern exchange of information, due to the lack of their own ICT capability, funding, etc.
- Lack of funding within the Justice Sector to fully and efficiently implement such delivery channels
- Deficiencies within the legal/administrative rules, restricting the ability to implement modern ICT tools across the sector and externally

Opportunities

- Price of new technologies and unit price of some capacities (i.e. storage) are decreasing,
- Governmental e-Government development efforts may provide additional resources
- Increased requests for e-Services from the public, from legal entities, from attorneys, from public notaries and private enforcers
- EU accession process opens new expectations and funds for developments

Threats

- Reluctance of other governmental agencies to establish electronic data channels
- Lower level regulatory items are missing (i.e. bylaws for Digital Signature) or are created very slowly
- Growing budgetary pressure and expenditure cuts

E.15. ENSURE VENDOR INDEPENDENT SERVICE ARCHITECTURE

E.15.1. RELEVANT PARTS OF DIAGNOSIS

Currently, the Justice Sector runs several different information systems within several different institutions. The existing information systems were designed using methodology and technology that is no longer suitable for

today's Justice Sector environment. Additionally, those information systems do not use many of the common Justice services functional and technical features and subsequently are potentially not as robust and secure.

The Ministry has, following the majority of requirements arising from the practice, already started the process of IT centralization. The Ministry has recognized this needs, and already started with the implementation of Case Management systems (SAPS, SAPO, SAPD and SAPA) within the largest institutions of the Justice Sector in Serbia (Courts, Prosecutors and Prison Administration). The systems are in the process of implementation (SAPA, SAPO) or deployment (SAPS). One of the main features of all three projects is common Enterprise Content Management platform – EMC Documentum, which could certainly allow for easier integration between the three institutions. The other feature of the projects is the request of the Ministry for the development and implementation of Enterprise Service Bus, which would positively improve and facilitate interoperability between the institutions. The still missing part of this set up is the development of messages structure and specifications.

However on the long run the feasibility of full roll-out of current solution heavily depends on the magnitude of licence and costs.

E.15.2. INTERNATIONAL TRENDS AND EU PRACTICE

International trends regarding the alignment of the business processes and Information Technologies and introduction of resilient and vendor independent ICT architecture of the Justice sector information systems vary within different countries based on the level of maturity of the systems. But, there is an approach common for almost all countries, the moving toward common IT architecture and introduction of flexible, loosely coupled components which could be easily interconnected, together with development of sets of data exchange standards.

Following examples of international trends and EU practice shows the intention of different justice organisations toward better business/IT alignment and resilient and vendor independent ICT Architecture:

- Using IT as a driver of modernisation within the justice system - IT solutions can simplify, improve and accelerate business processes (work sequences) in the courts, the state prosecutors' offices and the prison system. These objectives require changes to be made both in terms of work processes and in terms of IT solutions.
- Development of common solutions for the entire justice system is preferred to developing comparable and similar solutions for subsections of the justice system. Planning and decision-making in legal informatics, as well as development of IT solutions, are oriented to the enterprise architecture of the justice system, consisting of process architecture, solution architecture and governance processes. The enterprise architecture of the justice system is service-oriented (SOA).
- When selecting components of solutions, open source solutions should be considered by comparison with commercial software solutions. There is a whole host of advantages which offset the disadvantages of open source solutions such as functional obsolescence (no guaranteed further development by a manufacturer), the need to perform one's own maintenance and – experience has shown – less concern for reverse compatibility in the case of further developments. The advantages are: usually lower procurement costs, lower dependence on manufacturer's strategies, better adaptability and modifiability and less dependence on maintenance and updates by the manufacturer. Licence models of open source solutions should be precisely scrutinised as well, because they may entail far-reaching consequences. The decision between commercial software solutions and open source solutions should be made in the individual concrete case after undertaking a holistic review, taking account of economic aspects.

E.15.3. GOALS RELATED TO THE AREA

The overall business goal is to improve the ability of the Justice Sector to easily adopt any type of changes (organizational, legal, technical). This business goal is adaptable in ICT terms by setting up an architecture supporting the flexible changes of the IT systems and their connections.

Mid-level ICT goals

- Availability of proper and trusted information at proper time to authorised people to facilitate decisions
- Having supportive IT environment for automated information gathering and reporting
- Availability of Information Exchange Standards (between the judicial institutions, and cross-governmental exchange)
- Availability of a Central Registry for all IT systems of the Justice Sector
- End-users and staff members with deep knowledge on procedures are involved in IT developments
- Institutional processes are coordinated whenever new ICT systems are implemented / modified
- The Role of manual information exchange processes is reduced within the sector and with other actors
- During implementation of ICT system parallel development of the same functionality is eliminated

E.15.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- State of the art Case Management systems at some institutions
- New Case Management systems are developed on same platform
- Existing coordination of ICT development efforts

Weaknesses

- Fragmented case management systems, 3 separate ongoing implementations (SAPS, SAPO, SAPA)
- No information sharing standards defined on the semantic level
- ICT staff numbers too low, no specialization of ICT roles
- Lack of "user participation" in development projects
- Ministry budget is heavily constrained

Opportunities

- Price of new technologies and unit price of some capacities (i.e. storage) are decreasing,
- Increased requests for e-Services from the public, from legal entities, from attorneys, from public notaries and private enforcers
- Availability of international standards for regulation of various aspects of ICT developments and operations
- Knowledgeable business partners having accumulated deep knowledge of the justice ICT
- Access to qualified ICT staff on the local IT market

Threats

- Perpetual changes in the institutional framework of the Justice Sector
- Growing budgetary pressure and expenditure cuts
- Reluctance of other governmental agencies to establish electronic data channels

E.16. ENSURE VENDOR INDEPENDENT COMMUNICATION ARCHITECTURE

E.16.1. RELEVANT PARTS OF DIAGNOSIS

Currently within the Justice sector there are different WANs for the various parts of the sector (courts, AEPS, Ministry). Prosecutors do not have their dedicated WAN, they are using the access via the court network, with local virtual LANs in the same building.

WAN provision is outsourced to private vendors and to the Joint Services of the Republican Body agency. Network bandwidth is varying from 1Mbps to 30Mbps, and according to opinion of some institutions, the current capacities prohibit use of some ICT services (e.g. videoconferencing).

There are centralised network security services implemented, like virus protection, firewalls, authentication.

E.16.2. INTERNATIONAL TRENDS AND EU PRACTICE

Several Justice organisations around the world recognised that a stable communication architecture is a prerequisite for further efficiency improvement of the e-Justice infrastructure and thus significantly contributes to the overall improvement of judicial services. In most countries heavy investments were or are being made into development of communication architecture both on national level and on the level of the individual institutions.

The models are varying: at some countries wide area judicial communication networks are served by the government network or a dedicated judicial network in other countries the required WAN capacities are procured as services from local service providers. The selection between the different options is usually based on CAPEX/OPEX preferences and security concerns.

Reliability, security and availability issues are critical for provision of WAN and LANs, therefore at most countries certain redundancies and security related solutions are also considered.

E.16.3. GOALS RELATED TO THE AREA

Mid-level ICT goals:

- High availability of judicial ICT systems
- Performance of end-user environment supports everyday tasks
- High level, reliable ICT services for end-users
- Budget is in balance with operational costs

E.16.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- Well developed network infrastructure (WAN and local) at most sites
- Basic security measures have been taken (anti-virus, spam filtering)

Weaknesses

- No separate ICT infrastructure and ICT staff for prosecution offices
- Communication bandwidth is not wide enough at certain locations

Opportunities

- Price of new technologies and unit price of some capacities (i.e. storage) are decreasing,
- Knowledgeable business partners having accumulated deep knowledge of the justice ICT

Threats

- Growing maintenance costs as a result of donor-funded ICT developments and purchases

E.17. ENSURE VENDOR-INDEPENDENT INTEROPERABILITY AND INFORMATION EXCHANGE ARCHITECTURE

E.17.1. RELEVANT PARTS OF DIAGNOSIS

Currently the information exchange between the various institutions of the Justice sector are based on exchange of paper based documents. However this operational practice has become a significant obstacle of efficient and smooth processes.

Currently implemented Case Management Systems (SAP#) are based on Service Oriented Architecture and some interfaces, thus in theory they might be the foundation of an information exchange architecture.

E.17.2. INTERNATIONAL TRENDS AND EU PRACTICE

Interoperability is a central theme for the European Union at all public administration area including the Justice sector. From organisational viewpoint, interoperability appears on three levels:

- Interoperability within the justice institutions
- Interoperability within the justice sector
- Interoperability between justice sectors of different countries

Naturally EU puts heavy emphasis on the third level of interoperability as it is stated in “Towards a European e-Justice Strategy (COM(2008)329 final)”⁹ document as “The Commission will support national efforts and ensure that choices made regarding technology permit European interoperability.can be “.

but this can not be established without the developments of the first two levels. Virtually in all EU countries interoperability within the justice sector received focus during the recent years.

E.17.3. GOALS RELATED TO THE AREA

Mid-level ICT goals:

- Availability of proper and trusted information at proper time to facilitate decisions
- Availability of proper information for the participants of judicial processes
- Having supportive IT environment for automated information gathering and reporting
- Availability of information exchange standards (between the justice institutions and cross-governmental exchange)

⁹ Source: http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_civil_matters/jl0007_en.htm

E.17.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- State of the art Case Management systems at some institutions
- New Case Management systems are developed on same platform
- Existing coordination of ICT development efforts

Weaknesses

- Document exchange with counterparts is paper based
- No information sharing standards defined on the semantic level
- IT operations are fragmented (staff, procurement, maintenance)

Opportunities

- Possible synergies from the new ministry structure - Public Administration added to MoJ
- Continuing availability of donor funding to finance developments
- Governmental e-Government development efforts may provide additional resources
- Availability of international standards for regulation of various aspects of ICT developments and operations

Threats

- Perpetual changes in the institutional framework of the Justice Sector
- Reluctance of other governmental agencies to establish electronic data channels
- Lower level regulatory items are missing (i.e. bylaws for Digital Signature) or are created very slowly

E.18. GOOD BALANCE OF INTERNAL AND EXTERNAL SERVICES WITH EFFICIENCY IN MIND

E.18.1. RELEVANT PARTS OF DIAGNOSIS

Normal functioning of the Ministry and the judicial system, including performance of its core functions, are supported by units providing IT services. In the Ministry this is the Unit for e-Justice. The Unit in the Ministry is directly responsible for the implementation of the ICT projects within the whole Justice Sector. Other institutions have similar IT units. The main task of these units is the management (creation, deployment, maintenance and development) in the provision of IT services. Although some of the courts and institutions have their own IT-related projects, they are all in sync with the plan of the Ministry.

Some of IT activities, which require unusual human resources from the point of view of the core judicial functions, can be grouped in the form of services and outsourced to external suppliers/bodies (outsourcers). This applies mainly to performing activities related to Maintenance Services. Some activities in other phases of the IT services life cycle, such as Service Deployment and/or Service Improvement, could be outsourced as well. In this case, internal IT units in the judicial institutions would perform basic work in the management of IT services at a strategic level as well as coordinating, controlling and performing part of the activities of the other levels.

In the current situation of the Justice Sector, the following major services are fully or partially outsourced:

- Provision of wide area network
- LAN development and maintenance
- Provision of e-mail services

- Application system development and implementation
- Application system support
- End-user hardware equipment (servers, workstations, printers) maintenance

The major outsourcing partners are for WAN/LAN email Orion Telekom, and the vendors of Case Management Software (MEGA,C.E. ATOS), antivirus software (Smart), hardware suppliers (SAGA, Informatika)

One major weakness of the current IT operations is the highly fragmented nature of its organisation, which prohibits the employment of highly specialised staff members for some marginal fields of ICT.

E.18.2. INTERNATIONAL TRENDS AND EU PRACTICE

In difficult financial and political times, the public institutions welcome improvements in cash flow and public services mainly associated with the Introduction of information technologies. This is particularly important in Justice sector in countries in Central and Eastern Europe where the judiciary reform is almost exclusively financed by external programs. Since the external financing is realized mostly on a project basis, providing the necessary professional capacity from the funding beneficiaries is essential for the implementation of activities in due time.

Reasons for outsourcing

When a new major IT project is developed, the institutions often find themselves lacking the necessary IT expertise. This is due mostly to the fast-changing nature of information technology and government's competitive disadvantages in hiring and training skilled IT personnel.

Rather than building an in house professional capacity, the institutions can outsource some specific IT services to private vendors that can provide identical services at much lower unit costs and pay only for on-going services. Vendors are more flexible than governments when responding to changes in demands for specific IT skill sets.

The successful adoption of an outsourcing service involves institutions in making important decisions about the best mechanism for delivering their services to the community. Outsourcing is a management tool and should be approached in that manner. In letting an outsourcing contract, whether for the first time or as a renewal exercise, the first step is to determine the primary reasons for the outsourcing.

IMPORTANT! While outsourcing in many cases generates savings, in CEE countries the cost reduction however is often not the main reason. The institutions outsource mainly to acquire services unavailable in house, not to reduce cost.

The main areas for the use of external services are:

Project management outsourcing - This type of services 'exports' the project management process into responsibility of external vendor with proven and diverse experience in project administration and management.

Application outsourcing - The services include granting access to specific type of information or information flows to the employees of the client. In that way, the client saves on expenses associated with purchasing and maintenance of equipment, applications and other resources.

Outsourcing of IT Infrastructure, support and maintenance services - This type of service includes uninterrupted access to elements of the customers' IT infrastructure – servers, networks and communications, user computers, peripheral devices, and other specialized computer equipment. The vendor provides all required resources, both human and technical. For this type of services, the performance of the IT infrastructure is defined

and guaranteed by the selected service level. The expenses related to having in-house IT services are limited but there is high qualified support available, without any investments for training or staff retention.

Outsourcing of communication Infrastructure, support and maintenance services - The external vendor provides communication channels that allow the flawless data exchange among different client sites. In addition to the provided reliable infrastructure, the vendor provides infrastructure experts for communication performance monitoring.

Outsourcing of system integration - This type of service is essential for large scale projects that encompass entire organizations already having separate applications and databases in various departments and units. The system integrator examines the old, fragmented systems, facilitates systems migration, provides consolidation of IT services.

E.18.3. GOALS RELATED TO THE AREA

Mid-level ICT goals:

- High availability of judicial IT systems
- Outsourced and PPP services are financially well prepared and fair
- Availability of a pool of external experts with good knowledge on Justice sector
- Budget is in balance with operational costs

E.18.4. RELEVANT PARTS OF THE SWOT ANALYSIS

Strengths

- Well-developed network infrastructure (WAN and local) at most sites
- Partly modernized end-user working environment
- Experience of ICT staff in operation of judicial systems
-

Weaknesses

- ICT equipment partly outdated and should be replaced until the rollout of current case management developments
- ICT staff numbers too low, no specialization of ICT roles
- IT operations are fragmented (staff, procurement, maintenance)
- Lack of established performance measurement system for ICT

Opportunities

- Create institutional identity through unified vision of all judicial bodies
- Knowledgeable business partners having accumulated deep knowledge of the justice ICT
- Access to qualified ICT staff on the local IT market

Threats

- Perpetual changes in the institutional framework of the Justice Sector
- Growing maintenance costs as a result of donor-funded ICT developments and purchases
- Growing budgetary pressure and expenditure cuts
- Talented ICT professionals, well-trained experts / trainers may be drawn away to the private sector with a promise of better salaries and career paths

F. DETAILED ANALYSIS OF THE STRATEGIC ACTIONS

In the main part of the ICT Strategy Report the Strategic actions were described. This section contains a detailed analysis of the actions which demonstrates their preconditions, major steps, resource and timing estimations by the Consultant, recommended priorities, affected institutions and their estimated risks.

F.1. ESTABLISH PROFESSIONAL, SERVICE ORIENTED ORGANIZATION

F.1.1. ADAPT A SERVICE ORIENTED APPROACH IN PROVISION OF IT SERVICES FOR END-USERS

Preconditions of Strategic Action

- Establish centralised ICT organisation or unit
- Assembly of service catalogue for all services provided by ICT

Major steps of the Strategic Action

1. Establish Application support with well-defined roles and responsibilities, corresponding to the business landscape in the Justice sector
2. Define clear escalation criteria and procedures (clear instructions for service desk staff when a request cannot be immediately resolved by service desk personnel. Establish time thresholds to determine when escalation should occur based on the categorization/prioritization of the request or incident)
3. Implement necessary support software and tools for application support (registration, communication, dispatch and analyse all calls, reported incidents, service requests and information demands).
4. Train the ICT staff to increase communication problem solving skills and emphasis towards end-users.
5. Advise end-users of the existence of the service desk and the standards of service they can expect.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR*	between 50 and 250 man days	2 quarters

*) Without Service Desk implementation which is part of an other Strategic action.

Consultants' recommended priority of the Strategic Action

Either this Strategic action would affect all of the Justice sector end-users, it has to be implemented in line with the implementation of centralised ICT landscape/environment. This action contributes to some high level ICT goals, like "Ensure supportive working environment and high system availability", "Ensure ICT systems sustainability", "Ensure uniform capability of ICT services, tools and methods across the sector" and "Increase ICT proficiency of end users, ICT staff and decision makers through training". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Drive transformation to service orientation, definition of service provision processes
End-users from all institutions	Users of services

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Necessary conditions of service orientations (Service Desk, well defined ICT processes) are not met	Decreased end-user satisfaction Recurring problems not addressed	M	Prepare feasibility study and provide justification of the benefits and the need to establish service orientation.
End-users unaware of the procedures	Decreased end-user satisfaction	L	Disseminate criteria and procedures to the end users, provide training if needed.

F.1.2. ASSEMBLY OF A SERVICE CATALOGUE FOR ALL SERVICES PROVIDED BY IT

Preconditions of Strategic Action

- none

Major steps of the Strategic Action

1. Train a few ICT staff members to Service Management to obtain the necessary knowledge
2. Definition of ICT Services based on end-user perception and ICT staff knowledge
3. Establishment of a service catalogue for all services provided by IT
4. Definition of major characteristics of the ICT services

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR	between 50 and 250 man days	2 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action indirectly affects the whole Justice sector and contributes to some high level ICT goals, like "Ensure supportive working environment and high system availability", "Enhance ICT operations efficiency through performance measurement" and "Have a good balance of internal and external services having efficiency in mind". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Establishment of IT service catalogue
Institutions	Providing information regarding the current level and future needs for IT related services

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Service catalogue elements will be too technical	Service catalogue will not deserve its role as a clear communication to the end-users, and as a result they may have "irrational" expectations towards ICT	H	Use an "industry standard" framework for assembly of Service Catalogue

F.1.3. NETWORK WITH PEER ORGANISATIONS IN THE EU AND REGION AND USE EXPERIENCE FROM OTHER COUNTRIES THAT HAVE ALREADY SOLVED THE ORGANISATION OF THE ICT SECTOR IN THE JUDICIARY

Preconditions of Strategic Action

- none

Major steps of the Strategic Action

1. Find peer organizations
2. Establish communication
3. Organize joint events, study trips or twinning projects for exchange of experience

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20.000 EUR	Between 50 man days and 250 man days	1 quarter

Consultants' recommended priority of the Strategic Action

This Strategic action affects the ICT units and supports a few high level ICT goals, like "Retain and motivate high achieving ICT staff at all levels and reduce turnover" and "Establish a central sector-wide ICT organisation". The combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and funding

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
No foreseeable risks	-	-	-

F.2. ESTABLISH CENTRAL, WELL STRUCTURED, SECTOR WIDE UNIT OR ORGANISATION

F.2.1. IMPLEMENT AN AWARENESS CAMPAIGN WITHIN THE JUSTICE SECTOR ON THE IMPORTANCE OF THE ICT IN MODERN JUSTICE PROCESSES

Preconditions of Strategic Action

- Network with peer organisations in the EU and region and use experience from other countries that have already solved the organisation of the ICT sector in the judiciary

Major steps of the Strategic Action

1. Research the Judiciary ICT experiences in the region and the EU
2. Prepare a campaign goals, plan and expected results
3. Prepare the topics and choose the appropriate approach (forums, bulletins, workgroups, etc.)
4. Deliver the presentations, have feedback meetings with the decision makers

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20.000 EUR	Between 50 man days and 250 man days	1 quarter

Consultants' recommended priority of the Strategic Action

This strategic action affects the whole Justice sector and contributes to a few high level ICT goals like "Establish a central sector-wide ICT organisation" and "Increase ICT proficiency of end users, ICT staff and decision makers". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and funding
Institutions	Participation of business decision makers in forums

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack approval by the high level officials	Strategic goal failure	L	Use the overall judicial strategy to justify the needs for ICT organization that will bring more efficient management of the ICT processes and resources.
Not adequately trained internal staff for implementing an awareness campaign	The goals and contents of the campaign may not be properly communicated with the target audience	M	Involvement of qualified specialists in the preparation and execution of the campaign.
Not enough relevant information to be communicated to the target audience	Not all questions of the target audience may be answered	M	Performing a thorough research on similar experiences in the region and the EU. Involvement of adequate specialist on ICT in the judiciary.
Campaign without a "face".	The campaign will not have a focal point. The effects would be "diluted".	M	Choose and train a champion to lead the campaign and be the "face" of the ICT organization.

F.3. ENSURE SUSTAINABILITY THROUGH “SERVICE LIFE CYCLE MANAGEMENT”

F.3.1. PREPARE AND IMPLEMENT LONG-TERM FEASIBILITY STUDY AND TCO METHODOLOGIES FOR ALL ICT SYSTEMS

Preconditions of Strategic Action

- Establish central ICT unit or organisation which would prepare and set the Feasibility Study template and TCO methodology.

Major steps of the Strategic Action

1. Preparation of Feasibility Study template and methodology of implementation of the FS, that clearly describe key alternative actions
2. Determine the factors of TCO and preparation of TCO methodology
3. Train project managers and system analysis to FS and TCO methodologies
4. Implementation of Feasibility study for all planned systems
5. Implementation of TCO methodology on all current and future systems

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR	between 50 man days and 250 man days	2 quarters

Human resource needs are dependent on the number of ICT systems studied. When the methodology is developed, a first cut FS or TCO analysis may be done using around 20-40 man days depending on the complexity of the system.

Consultants’ recommended priority of the Strategic Action

This strategic action affects the whole Justice sector, since it would help establish a framework for decision making on all future ICT systems and enable sustainability. It is an action which would not take a huge effort and would have a huge effect for the sector. It contributes to some high level ICT goals, like “Ensure ICT systems sustainability”, “Ensure uniform capability of ICT services, tools and methods across the sector” and “Improve ability to raise funds for ICT and to efficiently manage available funds”. The combined effect is 4 on a scale of 1-4,

Affected organisations and their role

Institution	Role
ICT unit or organisation	Specify methodologies, implement methodologies
Budget holders	Approve, make decisions, plan and allocate budget
Different business stakeholders	Involved in methodology implementation

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level	Preventive actions

Risk analysis		Risk mitigation	
		(L/M/H)	
Inappropriate feasibility study template and methodology for implementation	Implementing solutions failing to meet requirements, perform as expected or integrate with existing infrastructure	M	Consider resources available for planned systems. Verify requirements of the business stakeholders. Make decision based on valid justification.
Inappropriate TCO methodology	Misspending of ICT investment, inappropriate pricing, no IT contribution to the business, budget not in line with the actual situation	M	Accurate and timely identification of budget variances Awareness raising for business and budget holders to understand benefits and costs of ICT

F.3.2. ESTABLISH CHANGE MANAGEMENT PRACTICES INTO IMPLEMENTATION PROJECTS AND REGULAR TWO-DIRECTIONAL INFORMATION FLOW BETWEEN ICT AND END-USERS

Preconditions of Strategic Action

- Establish central ICT unit or organisation be responsible for change management procedures and practices.

Major steps of the Strategic Action

- Develop, document and promulgate a change management framework that specifies the policies and processes, including:
 - Roles and responsibilities,
 - Classification and prioritization of all changes based on business risk,
 - Assessment of impact
 - Authorization and approval of all changes by the business process owners and IT,
 - Identify key stakeholders of changes
 - Tracing and status of changes
 - Impact on data integrity
- Establish and maintain version control all over changes.
- Implement roles and responsibilities that involve business process owners and appropriate technical IT functions. Ensure appropriate segregation of duties.
- Establish appropriate record management practices and audit trails to record key steps in the change management process. Ensure timely closure of changes. Elevate and report to management changes that are not closed in a timely fashion.
- Consider the impact of contracted services providers (e.g., of infrastructure, application development) on the change management process. Consider integration of organizational change management processes with change management processes of service providers. Consider the impact of the organizational change management process on contractual terms and SLAs

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20, 000 EUR	between 50 and 250 man days	2 quarters

Consultants' recommended priority of the Strategic Action

This strategic action affects the whole Justice sector, since it would help end users accept changes in the systems more easily, as well ICT to implement new systems more easily. It contributed to some high level ICT goals

like, “Ensure ICT systems sustainability”, “Ensure uniform capability of ICT services, tools and methods across the sector”, “Increase ICT proficiency of end users, ICT staff and decision makers through training”. The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Specify best practices, implement change management procedure
End-users	Involved in implementation of changes

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Inappropriate resources allocation	Stakeholders may receive not enough information, without their involvement resistance may arise against the changes	M	An agreed standardised approach for managing changes in an efficient and effective manner Formally defined expectations and performance measurement
Unauthorised changes	End users and other stakeholders are informed after changes are carried out, which might lead to confusion, errors or blocking of working processes.	L	Changes reviewed and approved in a consistent and coordinated way
No tracking of changes	ICT system capabilities and actual working processes may contradict to each other. It is not possible to identify root cause of technical problems	H	An agreed standardised approach for managing changes in an efficient and effective manner
Failure to comply with compliance requirements	Changes are managed ad-hoc, stakeholders may have a negative attitude towards ICT.	M	An agreed standardised approach for managing changes in an efficient and effective manner Formally defined expectations and performance measurement

F.4. ENSURE FULL GOVERNANCE THROUGH SERVICE PERFORMANCE MEASUREMENT

F.4.1. DEFINE EXACT PERFORMANCE MEASURES FOR EACH INDIVIDUAL GOAL OF THE ICT STRATEGY

Preconditions of Strategic Action

- none

Major steps of the Strategic Action

1. Establish a set of key metrics with a high insight-to-effort ratio (insight into achievement of goal compared to effort to capture the goal) that enables measurement of the achievement of process goals, resource utilization, output quality and throughput time to support improvement of the process performance and outcome.
2. Define relationships between outcome and performance metrics, and integrate them into the performance management system (e.g., balanced scorecard), where appropriate.

3. Establish specific targets for goals and performance drivers. Define how the data are obtained, including mechanisms to facilitate goals measurement (e.g., automated and integrated tools, templates).
4. Compare actual measurement to the target and take action for significant deviations.
5. For key goals, compare performance and outcomes against internal and external benchmarks, and consider the result of the analysis for process improvement.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR	less than 50 man days	1 quarter

Consultants' recommended priority of the Strategic Action

This strategic action is critical for successful implementation of the ICT strategy, if not implemented it wouldn't be feasible to follow the progress of the strategy implementation. This Strategic action affects the mainly ICT organisation and contributes to some high level ICT goals like "Enhance ICT operations efficiency through performance measurement", "Increase ICT proficiency of end users, ICT staff and decision makers" and "Improve ability to raise funds for ICT and to efficiently manage available funds". Its combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Defining performance measures, monitoring, implementing corrective actions
Business stakeholders (top management)	Accept and decide on performance measures, decide on corrective actions

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Not sufficient knowledge in the sector to set up right measures	Performance weaknesses remains and repeat themselves Lost opportunity for improvement Performance not recognised, de-motivating staff	M	Organize workshops, trainings for staff to define measures
Performance gaps not identified in a timely manner	Lost opportunity for improvement	M	Organize workshops, trainings for staff to define measures Set up a framework for monitoring of performances
Deviations not recognised and addressed	Failure to deliver business requirements	M	Set up a framework for monitoring of performances

F.4.2. DEFINE SERVICE LEVEL AGREEMENTS WITH THIRD PARTY VENDORS AND RENEW CONTRACTS

Preconditions of Strategic Action

1. Establish centralised ICT unit or organisation responsible for SLA approval and involved in SLA definition.

2. Establish Service desk responsible for monitoring of SLA objectives
3. Assembly of a service catalogue for all services provided by IT

Major steps of the Strategic Action

1. Ensure that the stakeholders from IT and the business negotiate, agree to and approve service requirements, and document and communicate their SLAs as appropriate. The format and contents include exclusions, commercial arrangements.
2. Define and formalize roles and responsibilities for each service supplier.
3. Assign relationship owners for all suppliers and make them accountable for the quality of service(s) provided.
4. Establish and document a formal communication process between the organization and the service provider.
5. Confirm that the SLA management process promotes, promulgates, measures (qualitative and quantitative) and monitors the SLA objectives.
6. Periodically review and assess supplier performance against established and agreed-upon service levels. Clearly communicate suggested changes to the service supplier.
7. Perform periodic reviews of the SLA objectives, effectiveness and efficiency, and report to the SLA stakeholders.
8. Improve or adjust SLAs based on performance feedback and changes to customer and business requirements.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR	between 50 and 250 man days	2 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole sector and contributes to some high level ICT goals, like: "Enhance ICT operations efficiency through performance measurement", "Ensure supportive working environment and high system availability" and "Have a good balance of internal and external services having efficiency in mind". The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Define SLA, approve, monitor SLA objectives
All institutions in the sector using third party services	Involved in SLA definitions, report incidents

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Badly formulated SLAs	Gaps between expectations and capabilities, leading to disputes Customers and providers not understanding their responsibilities Inefficient and costly operational	M	Define SLA framework, involve end-users in the definition of SLA

Risk analysis		Risk mitigation	
	service Failure to identify and respond to critical service incidents		
Supplier not responsive or committed to the relationship	Problems and issues not resolved Failure to meet customer service requirements Inadequate service quality	M	Describe the SLA objectives to the supplier, request for commitment to the service execution and maintenance

F.4.3. DEFINE AND IMPLEMENT TECHNICAL LEVEL PERFORMANCE MEASURES FOR INTERNAL SERVICES

Preconditions of Strategic Action

- Establish centralised IT unit or organisation to manage OLAs.
- Assembly of Service catalogue for all services provided by IT
- Create SLAs for third party services.

Major steps of the Strategic Action

1. Define a process to develop, manage, review and adjust OLAs.
2. Ensure that OLAs are in place that identify, document and explain how the services will be technically delivered to the end-users (to support the SLAs). Ensure that OLAs specify all technical processes that are utilised and the SLAs they support.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR	between 50 and 250 man days	2 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action has an indirect effect on the whole Justice sector, although the technical service levels (OLAs) are mainly serving the IT. This section supports a few high level ICT goals like, "Enhance ICT operations efficiency through performance measurement" and "Ensure supportive working environment and high system availability". Its combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Define OLA, align with SLA, explain to end-user institutions
All institutions using services	End-users of the service

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Badly defined OLAs, not meeting business requirements and not in line with SLAs	Failure to provide services Increase of incidents	M	Educate and involve end-users in the definition of OLAs. Develop framework of services, providing level of criticality of services which should be used for OLA definition
Badly established organisation of service desk	Inefficient and costly use of operational resources	M	Define clear roles of the Service desk staff Develop framework of services, providing level of criticality of services which should be used for OLA definition

F.4.4. DEFINE AND USE AN END USER SATISFACTION SURVEY TO ASSESS USER'S PERCEPTION ON ICT SERVICES

Preconditions of Strategic Action

- Defined SLAs and OLAs

Major steps of the Strategic Action

1. Identify the customers for each IT operational service and new solution, and determine their quality acceptance criteria. Capture quality acceptance criteria through short structured questionnaires from end-users.
2. Periodically obtain end-user views on the IT standards and practices to ensure that they meet end-user expectations.
3. Regularly monitor and review the quality management against agreed-upon acceptance criteria. Include feedback from customers, users and management. Respond to discrepancies in review results to continuously improve the quality.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR	less than 50 man days	1 quarter

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and supports a few high level ICT goals, like "Enhance ICT operations efficiency through performance measurement" and "Ensure supportive working environment and high system availability". The overall effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Develop questionnaire, execute surveys, analyse results
All institutions using ICT services	Providing results

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Inappropriate questionnaire	Failure to adequately understand end-user expectations Inappropriate priority given to different services Quality defects	M	Carefully develop questionnaires

F.4.5. IMPLEMENT A UNIFIED AND REGULAR REPORTING SERVICE FOR MANAGEMENT ABOUT THE MAJOR ICT PERFORMANCE MEASURES

Preconditions of Strategic Action

- Establish central ICT unit or organisation responsible for ICT systems performance
- Establish performance measurement system, SLAs, OLAs.
- Define and use end-user satisfaction survey

Major steps of the Strategic Action

1. Establish a board and executive reporting process, based on the performance monitoring framework, for regular, accurate and timely reporting on IT's contribution to the business by measuring achievement of IT goals, mitigation of IT risks and the usage of resources.
2. Design senior management reports to highlight key issues (positive and negative) generally relating to IT's contribution to the business and specifically to IT solution and service delivery capability and performance.
3. Consolidate results of IT performance measurement. Translate them into business performance impacts (positive or negative) and incorporate the results into standard periodic reports to the board. Clearly link IT performance measurement to business outcomes and identify how IT supports business strategy.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR	less than 50 man days	1 quarter

Consultants' recommended priority of the Strategic Action

This Strategic action affects mainly one organisation (the ICT itself), and contributes to a few high level ICT goals, like: "Enhance ICT operations efficiency through performance measurement" and "Increase ICT proficiency of end users, ICT staff and decision makers through training". The combined effect is 1 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Specification, Project management
All institutions	Specification, end-user testing, end-user trainings

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Badly established reporting service for management	Senior management doesn't understand the results Disconnect between management and IT Inability of senior management to direct and control key IT activities	M	Establish reporting service considering resources needed and the business objectives and goals supported

F.5. INTRODUCE SERVICE HELP DESK TO PROVIDE SUPPORT

F.5.1. ESTABLISH A PROFESSIONAL SERVICE DESK ON SECTOR LEVEL WITH CLEAR RESPONSIBILITIES OF FIRST LINE, SECOND LINE AND APPLICATION SUPPORT

Preconditions of Strategic Action

- Assembly of a service catalogue for all services provided by IT
- Establish of the ICT unit or organisation

Major steps of the Strategic Action

1. Specify requirements towards a Service Desk application and select vendor to implement it
2. Establishment of a Service Desk center within the ICT organization, equipped with the necessary technical resources and sufficient number of personnel having the necessary professional qualification
3. Develop procedures for Service desk
4. Providing training for local ICT staff for adequate identification of emerging problems

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 100,000 EUR and 500,000 EUR	between 250 man days and 1000 man days	3 quarters

Consultants' recommended priority of the Strategic Action

This Strategic Action affects the whole Justice sector and significantly contributes to several high level ICT goals, like "Ensure ICT sustainability", "Ensure uniform capability of ICT services...", "Ensure supportive working environment", "Enhance ICT operations efficiency..." and others. The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Establishment of Service Desk (selection and implementation of Service Desk application, development of internal procedures) Providing training for local ICT staff
All judicial institutions	Participation in Service Desk implementation and related trainings of local ICT staff

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Implemented Service Desk functions and procedures are too complex	Operation of implemented Service Desk is not full, therefore cases might be lost, performance data is not accurate	H	Focus on the most critical procedures (services) of the Service catalogue. Define simple priority and escalation rules. Clearly define roles of first and second level support
Lack of a central Service Desk personnel	Delays in troubleshooting requiring the central level intervention	M	Recruit staff from the talented local ICT staff of the Justice sector
Lack of qualified Human resources locally	Delays in troubleshooting requiring the local level intervention	M	Provide proper training for local staff.
Service Desk underperforms after implementation	Incident resolution takes more time than required	H	Clearly define first and second level support boundaries. Provide local resources for first level support (e.g. spare parts, toners, etc.) Provide proper training for support staff Establish mid-level repositories for items for quick replacements (e.g. some spare workstations, printers, routers, etc.)

F.6. ENSURE SUSTAINABILITY VIA PROPER FINANCIAL(BUDGET) MANAGEMENT

F.6.1. ESTABLISH A YEARLY DONOR CONFERENCE WHICH DEMONSTRATES THE RESULTS AND THE GOALS

Preconditions of Strategic Action

- none

Major steps of the Strategic Action

1. For each yearly conference select recently closed and ongoing projects and assign presenters for the major ones
2. Organise time and venue
3. Invite donor organisations (and media)

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR	less than 50 man days	1 quarter

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to a few high level ICT goals like "Improve ability to raise funds for ICT and to efficiently manage available funds" and "Increase ICT proficiency of end users, ICT staff and decision makers". The combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	High level representation
ITC unit or organisation	Organisation of the event
Selected institutions	Preparation of presentation on their key projects and results

Major risks

The top risks for the implementation of the Strategic action are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Disinterest of donor organisations or media	Few or low level participants having no influence on donor funding decisions	M	High level sponsorship at the Ministry Well placed communication of the event addressed at the top managers of donor organisations.

F.6.2. ESTABLISH ICT STRATEGY UPDATE RESPONSIBILITY WITHIN THE MINISTRY

Preconditions of Strategic Action

- none

Major steps of the Strategic Action

1. Evaluate the changing external and internal conditions
2. Determined the required changes
3. Modify the strategy components
4. Communicate the changes of the ICT Strategy

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20.000 EUR	between 50 and 250 man days	1 quarter

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to a few high level ICT goals like "Improve ability to raise funds for ICT and to efficiently manage available funds" and "Increase ICT proficiency of end users, ICT staff and decision makers". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Provide information on changing conditions and expectations Communicate the updated Strategy to donor organisations
ICT unit or organisation	Drive Strategy evaluation and updates
Delegated key institutions	Participate in strategy execution evaluation and strategy updates

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
- no foreseeable risk is identified	-	-	-

F.6.3. DEFINE A UNIFORM BUSINESS CASE STRUCTURE FOR ICT RELATED INVESTMENTS

Preconditions of Strategic Action

- none

Major steps of the Strategic Action

1. Develop a template for Business Cases and verify it with the other key organisational units of the Ministry
2. Define process and responsibilities for the Business Case preparations
3. Initiate a pilot Business Case for one or two projects
4. Evaluate the pilot and fine-tune the Business Case template

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20.000 EUR	between 50 and 250 man days	1 quarter

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to a few high level ICT goals like "Improve ability to raise funds for ICT and to efficiently manage available funds" and "Increase ICT proficiency of end users, ICT staff and decision makers". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Provide expectations and feedback on Business Case template Accept and announce Business Case template and roles/responsibilities associated with it
ICT unit or organisation	Prepare Business Case template and prepare pilot BCs for 1-2 projects.

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
- no foreseeable risk is identified	-	-	-

F.7. ENSURE HIGH QUALITY USER EXPERIENCE

F.7.1. DEVELOP TECHNOLOGY STANDARDS (FOR END-USER ENVIRONMENT)

Preconditions for the Strategic Action

- Establish of the ICT unit or organisation

Major steps of the Strategic Action

1. Select major areas of internal technical standardisation
2. Assess currently used technologies and future industrial trends
3. Propose technology standards and discuss it with key ITC stakeholders within the Justice sector
4. Accept technology standards

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20,000 EUR	between 50 and 250 man days	4 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to some high level ICT goals like "Ensure supportive working environment and high system availability", "Ensure uniform capability of ICT services, tools and methods across the sector" and "Provide sector wide knowledge sharing and access to relevant information". The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
Central ICT unit or organisation	Project management and implementation Definition of technology standards
MoJPA	Acceptance of technology standards
Selected ICT stakeholders	Review technology standards

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Defined technology standards are too restrictive	Certain requirements may not be satisfied	M	Review the technology standards regularly. Enable deviations from the technology standards, whenever it is verified

F.7.2. DEFINE PROFILES AND IMPLEMENT DESKTOP VIRTUALIZATION SOLUTION

Preconditions for the Strategic Action

- SRPS ISO/IEC 2700# and 20000 implementation and certification with other relevant standards should be performed

Major steps of the Strategic Action

1. The central ICT unit or organisation needs to prepare a feasibility study that will investigate the virtualization aspects to be used at the justice institutions
2. Defining profile users
3. Provision of adequate ICT hardware, networking and software infrastructure need
4. Implement desktop virtualisation at selected pilot sites
5. Evaluate the pilot and decide on the extension of the virtualisation

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 20,000 and 100,000 EUR	between 50 and 250 man days	2 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to a few strategic goals like "Ensure supportive working environment and high system availability" and "Ensure uniform capability of ICT services, tools and methods across the sector". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
The ICT unit or organisation	Prepares ICT hardware, networking and software infrastructure for the desktop virtualization Project management and implementation
MoJPA	Supervision of the project

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
End users rejects usage of desktop virtualization	Since virtualization sometimes does not allow to manipulate with files as same as with standalone workstation, users make a big pressure to stop usage of desktop virtualization	M	The ICT Policy Act for Serbian Judiciary should clearly state that usage of technologies specified by the central ICT body is mandatory in all judicial institutions. End users should be acquainted with all advantages of the desktop virtualization usage
Workstations configuration do not support installation of the virtualization software	New virtualization software installation on old PCs can significantly slow down performance of the PC	H	Old PCs should be replaced with new PCs.
Inadequate budgeting in regards to licensing for the virtualization software	Inadequate number of licenses for virtualization software could make insufficient solution that affect system performances	M	Good planning with outsourced consulting services in regards to virtualization licensing. Proactive attitude has to be shown in order to find funding from Serbian budget and/or donor organizations

F.8. ENHANCE SUPPORTIVE WORKING ENVIRONMENT

F.8.1. IMPLEMENTATION OF CASE MANAGEMENT SYSTEM AT REGULAR COURTS

Preconditions of Strategic Action

- Setting up a common data structure framework for court information publication.
- Set up a central location for public court document storage and access.
- Prepare and implement long-term Feasibility Study and TCO methodologies for all ICT systems.
- Establish sector-wide architecture management responsibilities to maintain a registry for ICT systems.
- Define common master data used for all systems
- Adapt and implement common ICT security methodology and procedures
- Develop and implement of Business Continuity plans and Disaster Recovery plans
- Define Service Level Agreements with third party vendors and renew contracts
- Review and strengthen authentication and authorisation methods
- Improve physical security of data centres, server rooms and other sensitive areas
- Establish dedicated test environments for all IT systems filled with depersonalised data
- Implement a comprehensive Training Register to support the whole training process

Major steps of the Strategic Action

1. Conduct a feasibility study for implementation of unified CMS in all regular courts
2. Make a decision on strategic approach
3. Seek for funds (e.g. mix of state budget funds, IPA funds and donor funds)
4. Initiate changes in the legal framework to accommodate effective use of electronic CMS
5. Upgrade judicial WAN infrastructure and ensure high-availability on all levels
6. Develop/upgrade selected system to accommodate all strategic goals
7. Conduct phased training and roll-out of selected
8. Manage implementation of the preferred system

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
More than 500.000 EUR	More than 1000 man days	6-8 quarters

Consultants' recommended priority of the Strategic Action

This strategic action is one of the most important and with greatest impact to court system. Due to its significant complexity, risk and funding requirements, it should be in the central focus of the Ministry of Justice and Public Administration and future ICT unit or organisation. This action contributes to several high level ICT goals like, "Improve functionality and coverage of ICT systems", "Ensure supportive working environment and high system availability", "Ensure uniform capability of ICT services, tools and methods across the sector" and "Ensure widely available web-based services for all users". The estimated combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals, co-funding and facilitating law changes
ICT unit or organization	Project management, end-user support
All regular courts	Active use of the system, providing feedback and suggestions.

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Obstacles in the legal framework	Inability to implement strategic action	H	Enacting changes in the laws and court rules of procedure, to support electronic content management and new delivery channels.
Insufficiently developed WAN infrastructure	Poor performing and unreliable system from users standpoint	H	Increase bandwidth and reliability of the judicial Wide Area Network.
Lack of appropriate funding	Inability to implement strategic action	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Inappropriate hardware and network equipment in the central computing location, or lack of high availability and redundancy.	Poor reliability and significant business continuity problems for entire court system	M	Involvement of highly qualified specialists in the hardware and network equipment specification; Building redundancy and high-availability in the hardware architecture;
Inappropriate software technology or architecture selected	Low functionality, reliability or performance	M	Involvement of highly qualified specialists in the evaluation of software technology stack; Incorporating end-users feedback into evaluation process.
Missing projected implementation deadlines	Strategic goal failure or significantly delayed implementation	H	Assigning qualified and experienced project managers in the ICT unit or organisation body to lead the effort;

F.8.2. IMPLEMENTATION OF CASE MANAGEMENT SYSTEM AT ALL PROSECUTOR'S OFFICES

Preconditions of Strategic Action

- Prepare and implement long-term Feasibility Study and TCO methodologies for all ICT systems.
- Establish sector-wide architecture management responsibilities to maintain a registry for ICT systems.
- Define common master data used for all systems
- Adapt and implement common ICT security methodology and procedures
- Develop and implement of Business Continuity plans and Disaster Recovery plans
- Define Service Level Agreements with third party vendors and renew contracts
- Review and strengthen authentication and authorisation methods
- Improve physical security of data centres, server rooms and other sensitive areas
- Establish dedicated test environments for all IT systems filled with depersonalised data
- Implement a comprehensive Training Register to support the whole training process
- Completion of the current SAPO implementation

Major steps of the Strategic Action

1. Evaluate the lessons learnt and finalize the system in accordance with end users feedback
2. Prepare Feasibility Study for Prosecutorial Case Management system implementation
3. Establish funding for the prosecutorial Case Management system
4. Select and contract vendor for Case Management implementation
5. Physically separate Basic Prosecutorial Offices' LANs from the court LANs on the locations where this is not done
6. Upgrade WAN infrastructure and ensure high-availability and sufficient bandwidth
7. Manage training and full roll-out of the system in all levels of prosecutorial offices
8. Secure the funding for long term maintenance of the system

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
More than 500.000 EUR	More than 1000 man days	8 quarters

Consultants' recommended priority of the Strategic Action

This strategic action is the most important for strategic development and increasing efficiency of the prosecutorial offices. It should be in the central focus of the Ministry of Justice and Public Administration and future ICT unit or organisation. This action contributes to several high level ICT goals like, "Improve functionality and coverage of ICT systems", "Ensure supportive working environment and high system availability", "Ensure uniform capability of ICT services, tools and methods across the sector" and "Ensure widely available web-based services for all users". The estimated combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals, co-funding and facilitating law changes
ICT unit or organisation	Project management, end-user support
Basic, Higher, Appeal and Republic prosecutorial offices	Active use of the system, providing feedback and suggestions. Participation in trainings, data load and migration

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Obstacles in the legal framework	Inability to implement strategic action	H	Enacting changes in the laws and bylaws, to support electronic document management.
Insufficiently developed WAN infrastructure	Poor performing and unreliable system from users standpoint	H	Increase bandwidth and reliability of the judicial Wide Area Network.
Lack of appropriate funding	Inability to implement strategic action	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Inappropriate hardware and network equipment in the central computing location, or lack of high availability and redundancy.	Poor reliability and significant business continuity problems for entire AEPS system	M	Involvement of highly qualified specialists in the hardware and network equipment specification; Building redundancy and high-availability in the hardware architecture;
Missing projected implementation deadlines	Strategic goal failure or significantly delayed implementation	H	Assigning qualified and experienced project managers in the ICT unit or organisation to lead the effort;

F.8.3. IMPLEMENTATION OF CASE MANAGEMENT AND RECORDS MANAGEMENT SYSTEM AT PRISON ADMINISTRATION

Preconditions of Strategic Action

- Prepare and implement long-term Feasibility Study and TCO methodologies for all ICT systems.
- Establish sector-wide architecture management responsibilities to maintain a registry for ICT systems.
- Define common master data used for all systems
- Adapt and implement common ICT security methodology and procedures
- Develop and implement of Business Continuity plans and Disaster Recovery plans

- Define Service Level Agreements with third party vendors and renew contracts
- Review and strengthen authentication and authorisation methods
- Improve physical security of data centres, server rooms and other sensitive areas
- Establish dedicated test environments for all IT systems filled with depersonalised data
- Implement a comprehensive Training Register to support the whole training process

Major steps of the Strategic Action

1. Evaluate the lessons learnt from SAPA implementation
2. Prepare Feasibility Study for AEPS system implementation
3. Establish funding for the AEPS system
1. Select and contract vendor for AEP Case Management and Records Management implementation
2. Secure funding for the long-term system maintenance
3. Upgrade WAN infrastructure and ensure sufficient bandwidth and high-availability
4. Test the system in several pilot-facilities, make necessary modifications as necessary
5. Manage phased training and roll-out of the system in all prisons

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
More than 500.000 EUR	More than 1000 man days	6 quarters

Consultants' recommended priority of the Strategic Action

This strategic action is one of the most important developments at the penitentiary branch of the Justice sector. Due to its significant complexity, risk and funding requirements, it should be in the central focus of the Ministry of Justice and Public Administration and future ICT unit or organisation. This action contributes to several high level ICT goals like, "Improve functionality and coverage of ICT systems", "Ensure supportive working environment and high system availability", "Ensure uniform capability of ICT services, tools and methods across the sector" and "Ensure widely available web-based services for all users". The estimated combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals, co-funding and facilitating law changes
ICT unit or organisation	Project management, end-user support
All institutions under the AEPS	Active use of the system, providing feedback and suggestions. Participation in trainings, data load and migration

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Obstacles in the legal framework	Inability to implement strategic action	H	Enacting changes in the laws and rules of procedure, to support electronic case management and new delivery channels.
Insufficiently developed WAN infrastructure	Poor performing and unreliable system from users standpoint	H	Increase bandwidth and reliability of the entire judicial Wide Area Network.
Lack of appropriate funding	Inability to implement strategic action	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)

Risk analysis		Risk mitigation	
Inappropriate hardware and network equipment in the central computing location, or lack of high availability and redundancy.	Poor reliability and significant business continuity problems for entire prosecutorial system	M	Involvement of highly qualified specialists in the hardware and network equipment specification; Building redundancy and high-availability in the hardware architecture;
Inappropriate software technology or architecture selected	Low functionality, reliability or performance	M	Involvement of highly qualified specialists in the evaluation of software technology stack; Incorporating end-users feedback into evaluation process.
Missing projected implementation deadlines	Strategic goal failure or significantly delayed implementation	H	Assigning qualified and experienced project managers in the ICT unit or organisation to lead the effort;

F.8.4. EXTEND FUNCTIONALLY CASE MANAGEMENT SYSTEMS (I.E. FULL ELECTRONIC CASE MANAGEMENT)

Preconditions of Strategic Action

- Case Management System implementation at all regular Courts
- Setting up a common data structure framework for court information publication.
- Set up a central location for public court document storage and access.
- Prepare and implement long-term Feasibility Study and TCO methodologies for all ICT systems.
- Define common master data used for all systems
- Adapt and implement common ICT security methodology and procedures

Major steps of the Strategic Action

1. Conduct a Feasibility Study for implementation of full-featured electronic document management systems in courts
2. Make a decision on necessary document management capabilities
3. Verify that legal framework supports effective use of electronic document management in courts, modify regulatory environment if need arises
4. Upgrade judicial WAN infrastructure and ensure high-availability on all levels
5. Conduct phased training and roll-out of upgraded document management functionalities

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
More than 500.000 EUR	More than 1000 man days	6 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the judicial branch of the Justice sector and contributes to some few level ICT goals like "Ensure supportive working environment" and "Ensure widely available web-based services for all users". The estimated combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals, co-funding and facilitating law changes
ICT unit or organisation	Project management, end-user support

Institution	Role
All courts	Providing initial document management requirements, Using of the system, providing feedback and suggestions.
Other institutions (if workflow integration is considered)	Define and implement common workflows

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Obstacles in the legal framework	Inability to implement strategic action	H	Enacting changes in the laws and court rules of procedure, to support electronic content management and new delivery channels.
Insufficiently developed WAN infrastructure	Poor performing and unreliable system from users standpoint	H	Increase bandwidth and reliability of the judicial Wide Area Network.
Lack of appropriate funding	Inability to implement strategic action	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Inappropriate hardware and network equipment in the central computing location, or lack of high availability and redundancy.	Poor reliability and significant business continuity problems for entire court system	M	Involvement of highly qualified specialists in the hardware and network equipment specification; Building redundancy and high-availability in the hardware architecture;
Inappropriate set of functionalities selected for particular court type	Detrimental work performance, dissatisfaction of users	M	Involvement of highly qualified specialists; Incorporating end-users requirements and feedback into implementation process;
Missing projected implementation deadlines	Strategic goal failure or significantly delayed implementation	H	Assigning qualified and experienced project managers in the ICT unit or organisation to lead the effort;

F.8.5. IMPLEMENTATION OF CASE MANAGEMENT SYSTEM IN THE MISDEMEANOUR COURTS

Preconditions of Strategic Action

- Setting up a common data structure framework for court information publication.
- Prepare and implement long-term Feasibility Study and TCO methodologies for all ICT systems.
- Establish sector-wide architecture management responsibilities to maintain a registry for ICT systems.
- Define common master data used for all systems
- Adapt and implement common ICT security methodology and procedures
- Develop and implement of Business Continuity plans and Disaster Recovery plans
- Define Service Level Agreements with third party vendors and renew contracts
- Review and strengthen authentication and authorization methods
- Improve physical security of data centers, server rooms and other sensitive areas

Major steps of the Strategic Action

1. Conduct a detailed feasibility study and compare total costs of ownership between several options for the misdemeanor courts CMS.
2. Secure financial funding (e.g. through co-funding with USAID JRGA project or EU/IPA projects)
3. Verify that legal framework allows for effective use of envisioned functionalities
4. Expand judicial WAN to cover all misdemeanor court seats and court units
5. Install LAN infrastructure in misdemeanor court buildings, where required
6. Initiate development and implementation
7. Monitor and control development and implementation of the misdemeanor CMS

8. Procure servers, storages and network equipment for the central server-farm in the Appellate court
9. Secure sustainable long term maintenance budget
10. Pilot the test in selected misdemeanor courts to verify that it satisfies users needs
11. Organize training and roll-out of the finalized system in all misdemeanor courts
12. Maintain the system

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 100.000 and 500.000 EUR*	More than 1000 man days	6-8 quarters

These costs cover only the initial implementation costs at the selected 6 pilot sites and do not cover the establishment of WAN to all 45 Misdemeanour courts, since depending on way of a third party service provider, majority of WAN costs might arise as operational costs.

Consultants' recommended priority of the Strategic Action

This strategic action is one of the most important and with greatest impact to court system. Due to its significant complexity, risk and funding requirements, it should be in the central focus of the Ministry of Justice and Public Administration and future ICT unit or organisation. This Strategic action affects one institution type and contributes to several high level ICT goals like "Improve functionality and coverage of ICT systems", "Ensure widely available web-based services for all users", "Ensure supportive working environment and high system availability" and "Increase ICT proficiency of end users, ICT staff and decision makers through training". The estimated combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals, co-funding and facilitating law changes
ICT unit or organization	Project management, end-user support
Misdemeanour courts and High Misdemeanour Court	Participation in specification, training Active use of the system, providing feedback and suggestions.

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Obstacles in the legal framework	Inability to implement strategic action	H	Enacting changes in the laws and court rules of procedure, to support electronic content management and new delivery channels.
Insufficiently developed WAN infrastructure	Inability to implement strategic action	H	Increase bandwidth and reliability of the judicial Wide Area Network.
Lack of appropriate funding	Inability to implement strategic action	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Inappropriate hardware and network architecture	Poor performance, reliability and significant business continuity problems	H	Involvement of highly qualified specialists in the hardware and network equipment specification; Building redundancy and high-availability in the hardware architecture;
Inappropriate software architecture	Low reliability or performance	M	Involvement of highly qualified ICT and field specialists in the evaluation of software and hardware technology stack; Incorporating end-users feedback into evaluation process.

Risk analysis		Risk mitigation	
Missing projected implementation deadlines	Strategic goal failure or significantly delayed implementation	H	Assigning qualified and experienced project managers in the ICT unit or organization to lead the effort;

F.8.6. INTEGRATION OF COMMERCIAL COURTS AND FUNCTIONAL IMPROVEMENT OF THEIR CASE MANAGEMENT SYSTEM

Preconditions of Strategic Action

- Setting up a common data structure framework for court information publication.
- Set up a central location for public court document storage and access.
- Prepare and implement long-term Feasibility Study and TCO methodologies for all ICT systems.
- Define common master data used for all systems
- Adapt and implement common ICT security methodology and procedures
- Develop and implement of Business Continuity plans and Disaster Recovery plans
- Review and strengthen authentication and authorisation methods
- Improve physical security of data centres, server rooms and other sensitive areas

Major steps of the Strategic Action

1. Conduct a feasibility study and calculate TCO for various scenarios
2. Make a decision on strategic approach
3. Specify functional and architectural improvement requirements
4. Seek for funds (e.g. mix of state budget funds, IPA funds and donor funds)
5. Upgrade judicial WAN infrastructure and ensure high-availability on all levels
6. Develop/upgrade selected system to accommodate all strategic goals
7. Conduct phased training and roll-out of selected system
8. Manage implementation

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
More than 500,000 EUR	More than 1000 man days	8 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects one institution type and contributes to few high level ICT goals like "Ensure widely available web-based services for all users", "Ensure supportive working environment" and. The estimated combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals, co-funding and facilitating law changes
ICT unit or organisation	Project management, end-user support
All Commercial courts	Active use of the system, providing feedback and requirements.

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Obstacles in the legal framework	Inability to implement strategic action	H	Enacting changes in the laws and court rules of procedure, to support electronic content management and new delivery channels.
Insufficiently developed WAN infrastructure	Poor performing and unreliable system from users standpoint	H	Increase bandwidth and reliability of the judicial Wide Area Network.
Lack of appropriate funding	Inability to implement strategic action	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Inappropriate hardware and network equipment in the central computing location, or lack of high availability and redundancy.	Poor reliability and significant business continuity problems for entire commercial court system	M	Involvement of highly qualified specialists in the hardware and network equipment specification; Building redundancy and high-availability in the hardware architecture;
Inappropriate software technology or architecture selected	Low functionality, reliability or performance	M	Involvement of highly qualified specialists in the evaluation of software technology stack; Incorporating end-users feedback into evaluation process.
Missing projected implementation deadlines	Strategic goal failure or significantly delayed implementation	H	Assigning qualified and experienced project managers in the ICT unit or organisation to lead the effort;

F.8.7. ASSET MANAGEMENT AND CASE MANAGEMENT SYSTEMS IMPLEMENTATION FOR DMSCA

Preconditions of Strategic Action

No preconditions are foreseen for this strategic action, except to ensure enough network bandwidth in order to have fully available solution to the DMSCA warehouse.

Major steps of the Strategic Action

1. Upgrade functionalities of the system in line with the business requirements.
2. Organize trainings for the staff for usage of the systems to the full extent.
3. Enable and provide interoperability with other Justice sector institutions.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 100,000 and 500,000 EUR	between 50 and 250 man days	1 quarter

Consultants' recommended priority of the Strategic Action

As this is the first "core business" information system, it would have significant impact for the work and process automation of the DMSCA and as well for other institutions exchanging information with DMSCA. This Strategic action affects one institution type of the Justice sector and contributes to some high level ICT goals like "Improve functionality and coverage of ICT systems", "Increase ICT proficiency of end users, ICT staff and decision makers through training" and "Ensure supportive working environment and high system availability". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
DMSCA	Preparations, project management and implementation activities

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Missing solution acceptance due to inappropriate change management practice	The staff would not use the solution	L	Train staff on the usage of the solution Management decision for the usage of the solution
Missing solution acceptance due to lack of maintenance resources	The staff would not use the solution	L	Fully include DMSCA IT organisation in the centralised ICT governance body
No interoperability in practice	No exchange of data with other institutions, more obligations for the staff (re-keying of data)	L	Set message exchange and interoperability standards

F.8.8. IMPLEMENT A PILOT MANAGEMENT INFORMATION SYSTEM ON CASE MANAGEMENT SYSTEMS TO PRODUCE UNIFORM ANALYTICAL SUPPORT

Preconditions of Strategic Action

- ICT unit or organisation to provide a definition of common data structure requirements for the sector-wide Management Information system

Major steps of the Strategic Action

- ICT unit or organisation to obtain Ministry's approval for the implementation of such pilot system, through several educational events and presentations to middle and top management
- Investigate all necessary pre-conditions for the implementation of such pilot (legal, procedural, technical, etc.)
- Consult with the vendors of various CMS systems in operation, determine most effective means of connecting them to the pilot and data exchange methods
- Define hardware, software, network, power, backup, functional and security requirements;
- Estimate costs, secure initial funding and sustainable budget for the future maintenance;
- Consult potential donors to obtain funding;
- Tender the development and implementation
- Select vendors and procure hardware, software and services;
- Setup and implement pilot management Information system;
- Review the results over a sufficient period of time; consider further steps, in obtaining a permanent solution.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 20,000 and 100,000 EUR	between 250 and 1000 man days	4 quarters

Consultants' recommended priority of the Strategic Action

This Strategic Action has effect on the whole Justice sector and contributes to a few high level Strategic goals, like: "Enhance ICT operations efficiency through performance measurement", "Ensure uniform capability of ICT services, tools and methods across the sector" and "Improve functionality and coverage of ICT systems". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Project management, review of results
Various selected institutions	Participation in requirement specification and in implementation

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Inappropriate technology, products or services selected	Insufficient level of functionality, reliability or performance	M	Involvement of qualified specialists in the evaluation and development of technical specifications.
Missing projected deadlines due to ineffective procurement process	Strategic goal failure	M	Avoiding procurements under provisions of Serbian Law on public procurement

F.9. ENSURE HIGH AVAILABILITY AND RELIABILITY

F.9.1. DEVELOP AND IMPLEMENT OF BUSINESS CONTINUITY PLANS AND DISASTER RECOVERY PLANS

Preconditions for the Strategic Action

- Establish the ICT unit or organisation
- Adoption of the ICT Policy Act for Serbian Judiciary where basic security rules should be stated

Major steps of the Strategic Action

1. Carry out a risk analysis of the major business processes within each institution types.
2. Develop templates for Disaster Recovery Plans and Business Continuity Plans
3. Determine the critical resources for the business processes and develop Disaster Recovery Plans for these resources.
4. Purchase/acquire equipment needed for the Disaster Recovery Plans (e.g. additional server capacities, spare workstations at central deposits)
5. Train ICT staff and test Disaster Recovery Plans in situations similar to real-life events.
6. Develop Business Continuity Plan for the most critical business processes
7. Purchase/acquire items needed for the temporary operations (e.g. preprinted forms)
8. Train business process participants to their role during temporary operations.
9. Test Business Continuity Plans in situations of unexpected events.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20,000 EUR*	between 50 and 250 man days	2 quarters

*) For most critical business processes and ICT equipment

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to some high level ICT goals, like "Ensure supportive working environment and high system availability", "Enhance Information Security" and "Provide sector wide knowledge sharing and access to relevant information". The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Defines methodology framework and templates for BPCs and DRPs. Define DRPs for most critical ICT systems. Project management and implementation
MoJPA	Supervision of the project
All Judicial institutions	Carry out risk analysis and determination of critical resources. Define temporary operations for unexpected events.

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
The procedures are not standardized	Any improvisation in the backup and disaster recovery procedures can cause that recovery could be not be accomplished at all	H	The ICT Policy Act for Serbian Judiciary should be operative in all judicial institutions. Strict usage of SRPS ISO/IEC 2700# and 20000 standards in all judicial institutions
Backup & Disaster Recovery procedures never tested in practice	Regular backup is regularly done but never followed with recovering the system from backup data. If backup was regularly done but on inappropriately way the recovery is in that way impossible because the backup data is not useful	H	The Backup and Recovery procedures should be tested regularly. The testing should be done at least once per year with full "from the scratch" recovery of the system
Inadequate hardware and software tools for backup data	Inadequate backup tools can cause problems in recovery of data in case of disaster	M	Proper planning should give right specification for software/hardware/telecommunication resources needed for backup and disaster recovery

F.9.2. SERVER CONSOLIDATION (VIRTUALIZATION)

Preconditions for the Strategic Action

- Establishment of ICT unit or organisation
- Data centre needs to be established
- Quality networking infrastructure is in function.

Major steps of the Strategic Action

1. Develop Feasibility Studies for server virtualisation effort – preferably linked to implementation or roll-out of centralised applications. Consider TCO calculations for the consolidated environment.
2. Determine required server capacities and expected future needs
3. Establish funds for the server consolidation (virtualization);
4. Prepare technical specification for virtualised server environment
5. Purchase and implement necessary equipment (possibly as part of software delivery projects)
6. Conduct implementation / server migration

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 100,000 and 500,000 EUR*	between 250 and 1000 man days	2 quarters

*) Although the initial costs are quite large, the savings during the lifecycle may be tremendous which should be validated by proper TCO calculations.

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to some high level ICT goals like “Ensure supportive working environment and high system availability”, “Ensure uniform capability of ICT services, tools and methods across the sector” and “Enhance Information Security”. The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Prepare Feasibility Study and technical plans for server consolidation. Specify ICT hardware, networking and software infrastructure for the server consolidation (virtualization): <ul style="list-style-type: none"> • Central data centre needs to be in production, • All software applications need to be “centralized” and to be run on the consolidated “central” servers; • Telecommunications links between the judicial institutions and central location (data centre) should have enough bandwidth; • Disaster and Recovery procedures should be in use.
All Judicial institutions	Strictly follow technical instructions made by the ICT unit or organisation

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of funding	In case of low bandwidth or poor server configuration in central data centre, server consolidation can affect poor performances to the end-users	H	Funding should be systematically planned and should lean on both Serbian budget and donors' funding
Some case management system applications remains to work on	Local servers remain in place, consolidation may not have all	M	All “business” applications in Serbian Judiciary should be set to work in Client-Server

Risk analysis		Risk mitigation	
"local" servers	the possible benefits since this would cause to maintain servers at different locations (as it is the case today)		centralized environment, where all servers should be physically placed in the central data centre

F.9.3. UPGRADE FOR NO-SINGLE-POINT OF FAILURE BY IMPLEMENTING NECESSARY REDUNDANCIES FOR SERVER COMPONENTS AND NETWORKS

Preconditions for the Strategic Action

- Adoption of the ICT Policy Act for Serbian Judiciary
- Business Continuity plans and Disaster Recovery plans should be in use in the Serbian Judiciary

Major steps of the Strategic Action

1. Secondary remote data centre location/premises should be provided;
2. Capacity planning should be made on basis of acceptable outage levels (aka "window of vulnerability")
3. Necessary applications, hardware + networking + power equipment and data telecommunications services should be procured;
4. The telecommunication services should be provided from telecommunications service providers possess robust and redundant network

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 100,000 and 500,000 EUR*	between 50 and 250 man days	8 quarters

*) The data centres may serve as temporary back-up centre for each other thus in calculation we used a lower estimation focusing on somewhat increased server capacity and increased telecommunication costs.

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to a few high level ICT goals like "Ensure high system availability" and "Ensure widely available web-based services for all users". The combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Project supervision Adequate remote premises for secondary data centre have to be provided
ICT unit or organisation	Project management and implementation Procures necessary hardware + networking + power equipment and data telecommunications services: <ul style="list-style-type: none"> • Primary data centre needs to be in production, • Secondary data centre needs to be in production • All software applications need to be "centralized" and to be run on the consolidated "central" servers; • Telecommunications links between the judicial institutions and central location (data centre) should have enough bandwidth with redundancy;

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Poor telecommunications service (telecommunications provider does not have redundant network)	Loss of service	M	The telecommunication services should be provided from telecommunications service providers possess robust and redundant network. The last mile line redundancy should be considered too where copper/fibre primary line should be backed up with another copper/fibre line physically separated from primary one (not placed in same trunks) or with wireless secured connection. The links from the judicial institutions and to data centres have to have enough bandwidth where bandwidth to data centres should be much bigger.

F.9.4. SET UP BACKUP CENTRE(S) AND MECHANISMS FOR OFF-SITE STORAGE FOR BACKUP DATA

Preconditions for the Strategic Action

- Adoption of the ICT Policy Act for Serbian Judiciary
- Business Continuity plans and Disaster Recovery plans should be in fully use in the Serbian Justice sector

Major steps of the Strategic Action

1. Backup remote data centre location/premises should be provided;
2. Necessary additional applications, hardware + networking + power equipment and data telecommunications services should be specified and procured;
3. Secure storage of off-site data must be resolved
4. Backup and restore processes should be defined, implemented and monitored

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 20,000 and 100,000 EUR*	between 50 and 250 man days	4 quarters

*) Considering only capacity improvement of existing data centers and not the building of a totally separate one.

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to a few high level ICT goals like "Ensure supportive working environment and high system availability" and "Enhance Information Security". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Supervision of the project implementation
ICT unit or organisation	Project management and implementation. Procures necessary hardware + networking + power equipment and data telecommunications services: <ul style="list-style-type: none"> • Primary data centre needs to be in production, • Backup data centre needs to be in production Periodically tests the quality of data by implementing backup and disaster recovery testing procedures

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Inadequate premises for backup data centre	Loss of service	M	Premises should have following characteristics: <ul style="list-style-type: none"> • Distance from the primary location should be enough to prevent that earthquake, fire and flood incidents situations on one locations affect the other data centre), • High quality power supply with back up for power supply equipment (UPSs and power aggregates), • High quality air conditioning,
Shortage of funding	Establishment of data centres could cost a lot and any shortage of funding could cause inappropriate data centres which does not fulfil business needs	H	Before start of project, budgeting needs to be assured. Funding should be provided from the Serbian budget and donors' organizations.

F.9.5. ACHIEVE DECENTRALISATION AND CONSOLIDATION BY USING E-GOVERNMENT “CLOUD COMPUTING” INFRASTRUCTURE

Preconditions of Strategic Action

- Establishment of governmental level Cloud computing platform and services

Major steps of the Strategic Action

1. Investigate judicial (infrastructure) services which are fit for “cloud computing”
2. Establish agreement with e-Government infrastructure “owners”
3. Enable migration of services from judicial infrastructure to cloud architecture
4. Migrate services

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 20,000 and 100,000 EUR	between 50 man days and 250 man days	4 quarters

By this action significant operation costs may be saved.

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to few high level ICT goals like "Ensure uniform capability of ICT services, tools and methods across the sector", "Enhance Information Security", and "Align Business processes and ICT system functions through resilient and vendor independent ICT architecture". The combined effect is 3 on a scale of 1.4.

Affected organisations and their role

Institution	Role
MoJPA	Investigate Cloud computing opportunities Agree on conditions of e-Government cloud usage Migrate services to new cloud environment

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Cloud computing infrastructure will not be reliable enough	Services depending on governmental cloud will be unavailable or slow	M	Careful capacity planning Service Level Agreement with cloud provider agency

F.10. ENSURE HIGH EFFICIENCY

F.10.1. DEFINE COMMON MASTER DATA USED FOR ALL SYSTEMS

Preconditions of Strategic Action

- Establishment of a central ICT unit or organisation
- Setting up a common data structure framework for court information publication

Major steps of the Strategic Action

1. Providing access to the regulations governing the procedures for data creation (digital IDs formation, formation of mixed identifiers, maximum length of identifiers for each data element ...)
2. Definition of mandatory master data set and format to be used in information systems
3. Definition of data source systems and mechanisms, how the source data is entered into the master data set.
4. Definition of data entry, update and archiving responsibilities
5. Specification of Master Data system functions together with interfaces
6. Tendering, selection of vendor and contracting
7. Implementation of Master Data database and interfaces to source and target systems
8. Training of data owners (aka data stewards) for their responsibilities

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 20,000 and 100,000 EUR	between 250 man days and 1000 man days	3 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to few high level ICT goals like "Ensure high efficiency" and "Enhance Information Security". The combined effect is 2 on a scale of 1.4.

Affected organisations and their role

Institution	Role
MoJPA	Master data set and master data format definition Update and improvement of the master data set
All judicial institutions (and other institutions involved in judicial processes)	Providing of information for regulations governing data creation

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of a unified master data definition	Difficult communication between the different systems and inability to introduce a unified data mining mechanism	H	Prepare a high level overall Data Model for the sector and determine data elements used by various ICT systems Prepare clear semantic definition of master data
Lack of information about regulations governing data creation	Limited opportunities for e-services introduction	H	Define clear processes for data entry, validation, modification and archiving for Master data

F.10.2. DEVELOP COMMON LOOK-AND-FEEL STANDARDS FOR ALL WEB PAGES OF THE SECTOR

Preconditions of Strategic Action

- none

Major steps of the Strategic Action

- Review of the current legislation concerning access to information (public, restricted, confidential), regulations on accessibility for the (visually) impaired
- Adoption of a resolution on the content that will be published
- Definition of a commonly used terminology on the web pages
- Definition and adoption of a unified concept for common look-and-feel standard for judicial web pages
- Elaboration and acceptance of a web page prototype according to the concept

It is worth to mention that this Strategic action does not alter / develops the web pages themselves, only prototypes.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR	between 50 man days and 250 man days	2 quarters

Consultants' recommended priority of the Strategic Action

Although this Strategic action affects the whole Justice sector, but its contribution to the strategic goals is only minor and indirect, According to evaluation it has low effect. The estimated combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Legal basis review, Concept preparation, Prototype supervision
All judicial institutions	Concept review and acceptance

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Extended period for decision making on the content that will be published	Delay in production of the concept for common look-and-feel standard	M	Involvement of institutions having imperative role in making such a decision
Lack of funds for development of new web pages and modification of existing	Delay in publication of unified web pages on the Internet	M	Timely funds planning

F.10.3. IMPLEMENT COMMON SOFTWARE FOR NON-CORE PROCEDURES OF ACCOUNTING, HR MANAGEMENT, ASSET MANAGEMENT

Preconditions of Strategic Action

- Sector-wide consultations, resulting in eventual establishment of the Common Software Investigation Committee
- Raising the interest for introduction of the common software solutions across the sector

Major steps of the Strategic Action

1. Establish a sector-wide committee, to investigate and propose the best, i.e. most efficient solutions for each one of these common applications/systems; the membership should also include external experts, both from the government and industry.
2. The committee conclusions/proposals should be taken to the top management, in order to determine the political and other top-level circumstances affecting the decision on priorities and feasibility for each component;
3. The new ICT sector-wide organization should be tasked with determining the specific ICT requirements for such systems: hardware, software, network, power, backup, functional and security requirements;
4. Using the resulting specific conclusions for each system/project, the donor community should be consulted, in order to propose realistic, widely accepted order of actions.

5. Estimate costs, secure initial funding and sustainable budget for the future maintenance;
6. Determine based on previous actions, the potential tender processes for the development and implementation.
7. Select vendors and procure hardware, software and services;
8. Implement common solutions.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 100,000 and 500,000 EUR	Between 250 and 1000 man days	12-18 months

Consultants' recommended priority of the Strategic Action

This Strategic Action affects the whole Justice Sector, and supports some high level ICT goals like "Ensure uniform tools across the sector", "Align business procedures and ICT functions" and "Improve functionality and coverage of ICT systems". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing initial actions, governing of the whole process
ICT unit or organisation	Project management, specifications, tendering, HW/SW estimates

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of appropriate funding, donor interest	Strategic goal failure	M	Provide clear, decisive and fact-supported conclusions about the effectiveness of common solutions; Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Lack of government support for sector-wide common applications solutions	Insufficient level of support in order to implement, ensure funding	M	Proselytize the usefulness and increased efficiency of these common solutions, provide projection of future integrations across the government

F.10.4. EXTEND THE DOCUMENT MANAGEMENT CAPABILITIES OF THE IMPLEMENTED DOCUMENT MANAGEMENT SYSTEM

Preconditions of Strategic Action

- Setting up a common data structure framework for court information publication.
- Set up a central location for public court document storage and access.
- Develop a proper authentication and authorization scheme for accessing published documents on the court portal.
- Consider all necessary legal changes required to implement proposed new ICT delivery channels in Justice Sector.
- Define technical standards for the implementation of new ICT delivery channels.

- Procure, develop and implement additional software elements/systems necessary to utilize the new ICT delivery channels.
- Include the additional delivery channels into common IT security methodology and procedures.

Major steps of the Strategic Action

1. Define required level of electronic content-management support and perform feasibility study to verify that legal framework is ready for electronic document and case management;
2. Investigate need for regulatory changes and prepare new regulations which allow electronic storage, handling and archiving of certain documents if necessary;
3. Perform gap analysis to estimate level of effort and costs;
4. Secure funding for software changes, WAN consolidation, professional scanners and the equipment for recording of hearings.
5. Manage implementation of extended document management support in the existing systems.
6. Procure additional services (WAN) and hardware equipment (scanners and recording systems). These activities and costs are covered by other Strategic actions.
7. Train the users in affected courts to use new functionalities

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 100,000 and 500,000 EUR	More than 1000 man days	4-6 quarters

Consultants' recommended priority of the Strategic Action

Full-featured electronic document management is a precondition for many strategic goals, including implementation of central court portal and electronic documents exchange between judicial and external institutions. The successful implementation of this action is critical and should be one of the top priorities for the ICT unit or organization and the MoJPA. This Strategic action affects the Judiciary branch of the Justice Sector and contributes to some high level ICT goals, like "Improve functionality and coverage of ICT systems ", "Ensure widely available web-based services for all users " and "Ensure uniform capability of ICT services, tools and methods across the sector". The combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding, preparation for needed regulatory changes
ICT unit or organisation	Project management, specification, vendor selection and training organisation
Selected courts	Participation in defining notification procedures and policies and in trainings

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Obstacles in the legal framework	Inability to implement strategic action	H	Enacting changes in the laws and court rules of procedure, to support electronic content and case management in courts.

Risk analysis		Risk mitigation	
Lack of professional-level scanners in the courts	Inability to effectively use electronic document management system	M	Proactive seeking for sources of funding (state budget, IPA project funds, donors).
Obstacles in the legal framework	Inability to implement strategic action	H	Enacting changes in the laws and court rules of procedure, to support electronic content management and new delivery channels.
Insufficiently developed WAN infrastructure	Poor performing document management system	H	Increase bandwidth and reliability of the judicial Wide Area Network.
Lack of appropriate funding for software changes	Strategic action failure	M	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Inappropriate hardware and network equipment in the central computing location, or lack of high availability and redundancy.	Poor reliability and significant business continuity problems	M	Involvement of highly qualified specialists in the hardware and network equipment specification; Building redundancy and high-availability in the hardware architecture;
Inappropriate software technology or architecture selected	Low functionality, reliability or performance	M	Involvement of highly qualified specialists in the evaluation of software technology stack; Incorporating end-users feedback into evaluation process.
Missing projected implementation deadlines	Strategic goal failure or significantly delayed implementation	M	Avoiding large-scale procurements under provisions of Serbian Law on public procurement (i.e. conducting high-risk and high-value procurements through EU/IPA and other donor projects).

F.10.5. ADAPT AND IMPLEMENT COMMON PROJECT MANAGEMENT METHODOLOGY

Preconditions of Strategic Action

- Establish the central ICT unit or organisation

Major steps of the Strategic Action

1. Select Project Management methodology to follow
2. Adoption of common ICT project management practices (organisation, roles, procedures, templates, document storage)
3. Define specialities of Project Management methodology for special projects (e.g. small projects / large projects; system implementation projects, etc.)
4. Design and implement project management tools
5. Pilot implementation in case of one selected project, evaluation of the pilot
6. Select and train project managers, project sponsors for the basics of the methodology

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 20,000 and 100,000 EUR	between 250 man days and 1000 man days	2 quarters

Consultants' recommended priority of the Strategic Action

This Strategic Action has an effect on the whole Justice sector. It contributes to some high level ICT goals like: "Ensure uniform capability of ICT services, tools and methods across the sector", "Enhance ICT operations efficiency through performance measurement", "Retain and motivate high achieving ICT staff at all levels and reduce turnover". Its combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Project management methodology selection, tailoring and acceptance
All judicial institutions	Participation in a project management

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Project methodology will be too complex to follow	Methodology will not be used during projects	M	Consider only the really important project procedures Pilot the methodology and adjust it according to results.
Lack of qualified local staff	Delays in projects implementation	M	Involvement of institutions having imperative role in making of decision for providing the necessary HR.

F.10.6. ADAPT AND IMPLEMENT COMMON ICT SECURITY METHODOLOGY AND PROCEDURES

Preconditions of Strategic Action

- Establishment of the central ICT unit or organisation.

Major steps of the Strategic Action

1. Select methodological approach and standards (e.g. ISO 2700#) to be followed and train key ICT staff members
2. Perform a high level ICT risk analysis
3. Elaboration and acceptance of ICT security regulations according to the selected standard
4. Adoption of common ICT security practices
5. Communicate security practices and procedures

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 20,000 EUR and 100,000 EUR	between 250 man days and 1000 man days	3 quarters

Consultants' recommended priority of the Strategic Action

This Strategic Action affects the whole Justice sector and contributes to some high level ICT goals, like: "Ensure uniform capability of ICT services, tools and methods across the sector", "Enhance Information Security", "Increase ICT proficiency of end users, ICT staff and decision makers through training". Its combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Provide governance and leadership Communication of the implemented security standard for all branches of the Justice sector.
ICT unit or organisation	Elaboration of ICT security regulations, train ICT staff
All judicial institutions	Adoption of common ICT security practices

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Delays in adoption of common ICT security practices	Increased level of risk of ICT security incidents	H	Involvement of institutions having imperative role in making of decision for adoption of common ICT security practices.
Defined ICT security practices will not be followed	ICT security incidents may happen in the future	M	Raise awareness of end-users by communication and sanctioning Implement control mechanisms

F.10.7. ADAPT AND IMPLEMENT COMMON ICT OPERATIONS AND MAINTENANCE ORGANISATIONAL ROLES AND PROCEDURES

Preconditions of Strategic Action

- Establishment of central ICT unit or organisation

Major steps of the Strategic Action

1. Selection of the applied framework or standard
2. Train key ICT personnel for the selected framework
3. Acquire external knowledge for procedure design and implementation
4. Define ICT procedures and roles to be implemented
5. Elaboration and acceptance of common unified job descriptions for the ICT personnel
6. Train ICT personnel
7. Adoption of common duties for the ICT personnel

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 20,000 and 100,000 EUR	between 250 man days and 1000 man days	3 quarters for elaboration, acceptance of common unified job descriptions for the ICT personnel

Consultants' recommended priority of the Strategic Action

This Strategic Action affects the whole Justice Sector and contributes to several high level ICT goals, like: "Ensure uniform capability of ICT services, tools and methods across the sector", "Ensure supportive working environment and high system availability", "Enhance ICT operations efficiency through performance measurement", "Increase ICT proficiency of end users, ICT staff and decision makers through training" and "Retain and motivate high achieving ICT staff at all levels and reduce turnover". The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Elaboration of common unified job descriptions for the ICT personnel
ICT unit or organisation	Selection of operational framework, standard. Definition of key ICT procedures, roles and responsibilities. Implement and communicate new operational procedures Train the local ICT staff
All judicial institutions	Adoption of common duties for the ICT personnel Participate in training of ICT staff

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Delays in adoption of duties for the ICT personnel	Reduced quality of ICT services	M	Involvement of institutions having imperative role in making of decision for adoption of common duties of ICT personnel.
Defined ICT procedures will not be followed by local ICT staff	Operational service levels may not be kept	H	Train local ICT staff Regularly audit local ICT operations

F.10.8. CONSOLIDATE DESKTOP PRINTERS AND IMPLEMENT PRINTING CONTROL WITH SOME SYSTEM FOR IDENTIFICATION (ID CARDS, ETC.)

Preconditions for the Strategic Action

- Adoption of ICT Policy Act for Serbian Judiciary where the printing procedure act should be stated.

Major steps of the Strategic Action

- Prepare Feasibility Study for printer consolidation
- Based on the Feasibility study, a decision must be made whether the printer consolidation investments may be financed by Ministry/donors or it is better to outsource the printer service to a vendor (with a fee based on the number of printed pages)
- A public procurement procedure should be initiated for purchase of network printers / total outsourcing of printing services for all judiciary institutions.
- After vendor/service provider selection, the equipment may be installed.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR	between 50 and 250 man days	1 quarter

Printer consolidation may be carried out gradually institution by institution considering the amortisation of existing desktop printers. There is a significant difference in CAPEX and OPEX ratio for full outsourcing and having own equipment. The above estimation is for the case when the Justice Sector relies on printing as a vendor service and not on its own equipment. This is mainly a financial issue, but the major change is the consolidation of printers.

Consultants' recommended priority of the Strategic Action

This Strategic action may affect the whole sector and contributes to a few high level ICT goals, like: "Ensure supportive working environment and high system availability" and "Have a good balance of internal and external services having efficiency in mind". The overall effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
Central ICT unit or organisation	Prepares the feasibility study for printing control mechanism in Serbian Judiciary. public procurement procedure for the printing outsourcing services. Project management and implementation
MoJPA	Supervision of the project
All Judicial institutions	Provide to the Central ICT unit or organisation all necessary data needed for printer consolidation and printing control processes (data of all existing printers – for each printer should be provided following data: type of printer, serial number, date of purchase of the printer, general condition of the printer, average number of papers printed on the printer on monthly level etc.) Project supervision and funding

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Improprate funding planning or poorly written tender documentation	Loss of printing outsourcing services	M	The procurement documentation should be clear and should considered following: <ul style="list-style-type: none"> The printing outsourcing partner should have enough financial, technical and human capability to provide service on national level, Penalty should be set in case of latency or impropriety service
Rejection of end-users to follow new established printing rules	Continuous printing documents that are not allowed to be printed	H	MoJPA adopts the printing procedures act which specifies procedures and penalties in case of not following the procedures

F.11. ENSURE INFORMATION SECURITY

F.11.1. DECLARE IT SECURITY RELATED ROLES AND RESPONSIBILITIES BY INTRODUCING AND CERTIFICATION OF THE STANDARDS SRPS ISO/IEC 27001 AND BY PREPARING AN INFORMATION SECURITY POLICY AND SECURITY PROCEDURES

Preconditions for the Strategic Action

- Adapt and implement common ICT security methodology and procedures according to SRPS ISO/IEC 27001

Major steps of the Strategic Action

1. Introducing and certification of judiciary institutions for standard ISO /IEC 27001 and determine high level IT security principles and prepare a comprehensive Security Policy
2. Publish Security policy and forward it to every staff members (who have access to ICT equipment)
3. If possible that obtain signature from each employees about his/her acknowledgement of the Security Policy
4. Determine the roles of employees in ICT security procedures (of Strategic action 4.7) and train relevant employees for the procedures

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20.000 EUR	between 50 and 250 man days	2 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to a few high level ICT goals like "Enhance Information Security" and "Ensure uniform capability of ICT services, tools and methods across the sector". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Supervision of the project implementation
ICT unit or organisation	Introducing and certification of judiciary institutions for standard ISO /IEC 27001 and prepare Information Security Policy and define roles for security procedures Project management and implementation
Institutions	Staff members to get acquainted with Information Security Policy

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Rejection or negligence of end users to follow information security procedures	Security incidents	H	MoJPA needs to introduce and certify standard SRPS ISO/IEC 27001 for high level institutions and adopt the ICT Policy Act for Serbian Judiciary (information security policy and security procedures should be integral part of the act) and should officially send it to all employees in the Serbian Justice sector The central ICT unit or organisation needs to prepare draft of the ICT Policy document and send it for approval to the MoJPA The ICT unit or organisation should warn (trainings and workshops) all employees in the Serbian Justice about the importance of the information security

F.11.2. ESTABLISH A SOFTWARE LICENSE DATABASE

Preconditions for the Strategic Action

- none

Major steps of the Strategic Action

1. Establishment of central database of software licenses
2. Manual or automatic scan of workstations and servers
3. Optional elimination of non wanted or unlicensed software
4. Optional definition of software request/authorisation processes

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20.000 EUR*	Between 250 and 1000 man days	2 quarters

*) The above estimations do not cover the purchase of missing software licenses

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to a few high level ICT goals like "Enhance Information Security" and "Ensure uniform capability of ICT services, tools and methods across the sector". The combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Supervision of the project implementation
The ICT unit or organisation	Procures necessary software licensing database application Project management and implementation (scan and data entry into database) (Optional) elimination of unlicensed software, (optional) definition of software request/authorisation processes

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Use of illegal (unlicensed) software in the Serbian Judiciary	Non compliance with laws	M	The MoJPA should officially inform all Serbian judiciary institutions that all requested data in regards to software licenses should be sent to the ICT unit or organisation The central ICT unit or organisation should procure software solution that could automatically track status of installed software for each computer in the network
Individual purchasing of software licenses	Increased costs of software licenses		Centralized procurement of software licenses.

F.11.3. IMPLEMENT IDENTITY MANAGEMENT FUNCTION WITHIN THE IT ORGANISATIONS TO REVIEW END-USER ACCESS TO SOFTWARE FUNCTIONS

Preconditions for the Strategic Action

- SRPS ISO/IEC 27001 and SRPS ISO/IEC 20000 implementation and certification with other relevant standards should be performed

Major steps of the Strategic Action

- Establishment of the central user repository/directory
- Determination of needed software functions and data for the various job positions
- Specification of Identity Management system requirements and selection of appropriate tool
- Definition of Identity Management procedures
- Necessary software and hardware procurement
- Implementation of IDM tool and procedures

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 20,000 and 100,000 EUR	Between 250 and 1000 man days	5 quarters

*) The above costs are valid only for the basic Identity Management system costs with limited automatic interfaces to the authentication modules of the applications (only which are using LDAP protocol)

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to a few high level ICT goals like "Enhance Information Security" and "Ensure uniform capability of ICT services, tools and methods across the sector". the combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Supervision of the project implementation
The ICT unit or organisation	Define Identity Management processes Determine user roles and required access rights Procure necessary hardware and networking equipment Project management and implementation
Institutions	Active use, providing feed back

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Too complex authorisation structure (with a lot of special user roles)	Determination of access rights is virtually employee by employee, which leads to very long implementation time	H	Simplify user roles
Technical difficulties when building interfaces between IDM and application systems	Increased time and resource needs	M	Link only systems to IDM which support technical standards like LDAP

F.11.4. DEVELOP CAPACITIES TO ANALYSE TRANSACTIONAL LOGS

Preconditions for the Strategic Action

- Centralization of the servers should be performed

Major steps of the Strategic Action

1. Specify the requirements for log analysis
2. Assess the market and select log analyser (if text editor tools do not satisfy the requirements)
3. Develop internal processes to store logs at secure sites
4. Modify logging practices for the selected system components (setting extent of logging, protecting log file from deletion/modification)
5. Providing training for analysing transactional logs,
6. Providing tools for analysing transactional logs,

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20.000 EUR*	Less than 250 man days	One quarter

*) In case of freeware log analyser

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and supports a few high level ICT goals like "Enhance Information Security" and "Increase ICT proficiency of end users, ICT staff and decision makers through training". Th combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Supervision of the project implementation
The ICT unit or organisation	Procures necessary hardware and software tools Arrange trainings for selected employees Define processes and rules for transaction logging and analysis Project management and implementation

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Some applications may not keep and provide adequate logs	Inability to resolve incidents	M	Upgrade applications to generate specified level of details in the transactional logs
Overcomplicated log generation, too much information	Log sizes become very large, analysis with simple tools is not possible	M	Keep logging at an optimal level (only the critical events are to be logged)

F.11.5. REVIEW AND STRENGTHEN AUTHENTICATION AND AUTHORISATION METHODS

Preconditions for the Strategic Action

- SRPS ISO/IEC 2700# and 20000 implementation and certification with other relevant standards should be performed
- Declare IT security related roles and responsibilities by preparing an Information Security Policy and Security procedures

Major steps of the Strategic Action

1. Determine critical resources to protect (data, documents, system functions, components)
2. Deploying and managing secured identities via strong authentication/authorization methods, the use of encryption and digital signatures, etc.
3. Develop internal procedures and rules to strengthen authorisation and authentication (forced password changes, approval process for access right requests).
4. Providing a secure framework for delivering identity management from a tool and administrative perspective as well as from a "secure identity" perspective.
5. Communicate the new rules for the staff members.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 20.000 and 100,000 EUR*	between 50 and 250 man days	4 quarters

*) These costs do not cover a sector wide implementation of strong physical mechanisms (electronic ID cards and entrance systems), since they are handled by Strategic action 8.6. It also does not cover the authentication for the external web-pages for third party professionals (e.g. advocates), since it is handled in Strategic action 2.3.

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes some high level ICT goals like "Enhance Information Security", "Increase ICT proficiency of end users, ICT staff and decision makers through training" and "Ensure uniform capability of ICT services, tools and methods across the sector". the combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Supervision of the project implementation.
The ICT unit or organisation	Determine critical ICT resources to protect Develop internal procedures Specify authentication methods and tools to implement Procures necessary hardware and software (e.g. smart cards). Organize user trainings. Project management and implementation.

Major risks

The top risks for the implementation of the program are the following:

Risk analysis	Risk mitigation
---------------	-----------------

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of appropriate funding	Strategic goal failure	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Inappropriate technology, products or services selected	Insufficient level of functionality, reliability or performance	M	Involvement of highly qualified specialists in the development of technical specifications and evaluation of proposals.
Missing projected deadlines due to ineffective procurement process	Strategic goal failure	M	Assigning qualified and experienced project managers in the central ICT unit or organisation to lead the effort;

F.11.6. IMPROVE PHYSICAL SECURITY OF DATA CENTRES, SERVER ROOMS AND OTHER SENSITIVE AREAS

Preconditions for the Strategic Action

- SRPS ISO/IEC 2700# and 20000 implementation and certification with other relevant standards should be performed
- Declare IT security related roles and responsibilities by preparing an Information Security Policy and Security procedures
- Centralization of the servers should be performed

Major steps of the Strategic Action

1. Identify locations for critical application and data centres
2. Perform a risk analysis on the current facilities and determine minimal physical security requirements for each location types.
3. Implement physical security measures at selected locations, according to SRPS ISO/IEC 2700# standards and the defined security requirements

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 100,000 and 500.000 EUR	between 50 and 250 man days	4 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole justice sector and contributes to a few high level ICT goals like "Enhance information security" and "Ensure supportive working environment and high system availability". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Provides locations for data centres, Provides security staff, Provides funding Supervision of the project implementation.
The ICT unit or organisation	Definition of security requirements Procures necessary equipment Definition of security procedures Project management.

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of appropriate funding	Strategic goal failure	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Insufficient security measures	Loss and leakage of information	H	Strictly follow SRPS ISO/IEC 2700# standards related to physical security

F.11.7. RAISE THE AWARENESS OF STAFF ON IT SECURITY ISSUES BY DEVELOPMENT OF AN INTERNAL COMMUNIQUÉ

Preconditions of Strategic Action

- Establishment of central ICT unit or organisation for the Justice Sector
- Introduce and certify institutions of justice sector for standards SRPS ISO/IEC 27001, declare IT Security Roles and responsibilities by preparing an Information Security Policy and Security procedures
- Review and strengthen authentication and authorisation methods

Major steps of the Strategic Action

1. Determine major risks and adapt common ICT security control practices for end-users
2. Elaboration and acceptance of internal communiqué for common ICT security control mechanisms and sanctioning
3. Publish internal security communicate for every end-user

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20,000 EUR	Between 50 man days and 250 man days	2 quarters

Consultants' recommended priority of the Strategic Action

This strategic action affects the whole Justice sector and contributes for realisation of high level strategic goals like Enhance Information Security, Increase ICT proficiency of end-users and Ensure uniform tools and methods across the sector. The estimated combined effect of the Strategic Action is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Elaboration, acceptance and publication of internal communiqué for common ICT security control mechanisms and sanctioning.
All judicial institutions	Adoption of common ICT security control practices

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level	Preventive actions

Risk analysis		Risk mitigation	
		(L/M/H)	
Delays in adoption of common ICT security control practices	Increased level of risk of ICT security incidents	M	Involvement of institutions having imperative role in making of decision for adoption of common ICT security control practices.
Non-adherence of end-users to the published security measures	Breach of information security	H	Establishment of control activities (e.g. internal audits, restriction of end-user rights, continuous awareness-raising)

F.11.8. ESTABLISH DEDICATED TEST ENVIRONMENTS FOR ALL IT SYSTEMS FILLED WITH DEPERSONALISED DATA

Preconditions of Strategic Action

- Server consolidation (virtualization)

Major steps of the Strategic Action

1. Determine performance and technical requirements for dedicated test environments
2. Design architecture of test environment
3. Procure necessary software and hardware components
4. Implement hardware (if needed) and software components
5. Select, depersonalise and migrate data needed for particular tests
6. Define "Release procedures" governing all system changes and covering tests, communication, documentation, roll-out, trainings,

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 100,000 and 500,000 EUR	between 250 and 1000 man days	2 quarters

If the dedicated test environments are permanently maintained for a given system (because of relatively frequent system changes), then it implies further operational and maintenance resources.

Consultants' recommended priority of the Strategic Action

This Strategic Action has direct effect on only the ICT operations (indirectly it may affect the whole sector, since data protection and system reliability is improved by it). It contributes to a few high level ICT goals, like: "Enhance Information Security" and "Ensure ICT systems sustainability". Its combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Specification and design of test environment(s) Procurement of necessary components Implement hardware and software components (with vendor involvement) Maintenance, update and improvement of the test environment
Some selected institutions	Providing of information for regulations governing data creation Participation in data preparation, depersonalisation and migration

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of information about regulations governing data creation	Limited testing opportunities	H	Involvement of institutions having imperative role in making of decision for providing the necessary information
Selected, migrated and depersonalised data will not cover all future testing needs	Additional data load is needed	L	Carefully plan initial data, consider all possible data configurations

F.11.9. DEFINE COMMON TECHNICAL SECURITY REQUIREMENTS FOR ALL INFORMATION SYSTEMS, DATA TRANSMISSION, AUTHENTICATION

Preconditions of Strategic Action

- Declare IT security roles and responsibilities
- Review and strengthen authentication and authorisation methods

Major steps of the Strategic Action

1. Definition of data classification categories
2. Elaboration and acceptance of ICT technical security requirements
3. Investigation of current ICT systems and vendor contracts from technical security viewpoint
4. Introduction of common ICT technical security requirements

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20,000 EUR	between 250 man days and 1000 man days	2 quarters

Investigation and definition of technical security standards may require external specialist.

Consultants' recommended priority of the Strategic Action

This Strategic Action affects the whole Justice Sector and support a few high level ICT goals, like: "Enhance Information Security" and "Ensure uniform capability of ICT services, tools and methods across the sector". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Definition of data classification categories Acceptance of common ICT technical security requirements
ICT unit or organisation	Elaboration of common ICT technical security requirements Investigation of current ICT systems and vendor contracts
All judicial institutions	Adoption of common ICT technical security requirements

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Current information systems do not satisfy the defined technical security requirements	Extra resources are needed to meet the requirements	M	Define realistic (but not too relaxed) requirements
Delays in adoption of common ICT technical security requirements	Increased level of risk of ICT technical security incidents	H	Involvement of institutions having imperative role in making of decision for adoption of common ICT technical security requirements. Provide funds for improvement of security

F.12. INCREASE KNOWLEDGE AND PROFICIENCY

F.12.1. IMPLEMENT A COMPREHENSIVE TRAINING REGISTRY TO SUPPORT THE WHOLE TRAINING PROCESS

Preconditions of Strategic Action

- Reform of the Judicial Academy structure, modus operandi and systematization of positions (new *Sistemizacija*)
- Competent staff within the Judicial Academy to lead the process of these changes and enhancement of the Training process
- Political will and understanding of the need for modernization of the training process within the Sector's top management

Major steps of the Strategic Action

1. Identify the specific functional and technical needs for such a new system (Training Registry);
2. Identify necessary links between Training Registry and other relevant systems (Training portal, various databases containing staff information, HR systems, financial systems, etc.)
3. Define hardware, software, network, power, backup, functional and security requirements, leading to estimated costs, secure initial funding and sustainable budget for the future maintenance;
4. Ensure sufficient funding for the Training Registry project, including potential donors, based on clearly defined needs, i.e. definition of a problem, costs, solution and advantages;
5. Tender the development and implementation;
6. Select vendors and procure hardware, software and services;
7. Setup and implement the Training Registry.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 20,000 and 100,000 EUR	between 50 and 250 man days	4 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action mainly affects one institution and contributes to a few high level ICT goals like "Increase ICT proficiency of end users, ICT staff and decision makers through training" and "Improve functionality and coverage of ICT systems", The combined effect is 1 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Project management, implementation
Judicial Academy	Providing business directions, functional specifications

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of appropriate funding	Strategic goal failure	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Inappropriate technology, products or services selected	Insufficient level of functionality, reliability or performance	M	Involvement of highly qualified specialists in the development of functional and technical specifications and evaluation of proposals.
Missing projected deadlines due to ineffective procurement process	Strategic goal failure	H	Well prepared specification and evaluation criteria

F.12.2. STANDARDISATION AND INCREASE LEVEL OF DIGITAL LITERACY OF ALL EMPLOYEES

Preconditions of Strategic Action

- Establish a scheme and written principles for ICT related trainings for the sector

Major steps of the Strategic Action

- Select competence areas of digital literacy in line with internationally recognised programmes and standards (e.g. ECDL)
- Assess level of digital literacy for all employees
- Organise training programmes and acquisition of digital literacy certificates

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
More than 500,000 EUR	More than 1000 man days	24 months

*) Above cost can be significantly reduced if only training is limited and certification is fully supported.

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice Sector and has direct contribution to high level strategic goals of "Increase ICT proficiency of end-users, ICT staff...". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and funding or co-funding, project management, organisation and execution of assessment, training programme and certification

Institution	Role
Judicial Academy	Providing general training related knowledge and training infrastructure
All institutions	Participation in digital literacy assessment, trainings

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Training infrastructure is not prepared to train thousands of potential trainees	Full training process will be very long	H	Tight scheduling of trainings. Involvement of external trainers
Trainings will require extremely large amount of time and expenses	Training budgets will not be available for the whole training process	H	Have a good balance of available funds and training curricula
Resistance from staff members with less affinity to ICT	Very strong movements against training programme, lobbying at high levels	H	Gradual implementation of the programme, carefully designed internal communication, Support of training participants with dedicated working time for trainings

F.12.3. ESTABLISH A SCHEME AND WRITTEN PRINCIPLES FOR ICT RELATED TRAININGS FOR THE SECTOR

Preconditions of Strategic Action

- As for general preconditions: the establishment of the central ICT unit or organisation and the structure reform of the Judicial Academy (new *Sistematizacija*)
- Relevant human resources within the Judicial Academy to lead the whole systematic, logical and structured process, to implement the ICT training

Major steps of the Strategic Action

1. Identify the general ICT training needs, with participation of the wide representative group of the employees of the Justice sector and by using questionnaires and interviews.
2. Create written principles about the ICT training target groups, training topics, training methods, trainers, costs and other relevant issues.
3. Develop the new, comprehensive ICT training program for various target groups, to meet their training needs and develop training curricula, training materials.
4. Integrate the ICT training plan into the annual training plan of the Justice sector, taking into account the outsourced ICT trainings (for end-users, related to specific IT systems) and the annual ICT conference for the whole Justice sector as well.
5. Develop electronic tools for distribution of the training materials, including for everyday online access of guidelines and manuals.
6. Implement the Train-the-Trainers approach on ICT training, by identifying the core group of prospective trainers among the employees with ICT and/ or pedagogical knowledge, skills and experience, by further training and coaching them about pedagogical competences and by developing the motivation system for trainers.
7. Monitor and evaluate the ICT training activities, including the performance of trainers.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20,000 EUR	Between 50 and 250 man days	15 months

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice Sector and has direct contribution to high level strategic goals of "Increase ICT proficiency of end-users, ICT staff...". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and funding or co-funding
Judicial Academy	Project management, pedagogical and training organizer know-how
ICT unit or organisation	Content know-how
All institutions of the Justice sector	All employees as participants of the trainings, and as prospective trainers

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Low commitment of the prospective trainers	Trainings do not take place or delay	M	Development of precise action and monitoring plan. Creation of the motivation system for trainers
Lack of cooperation between Ministry and Judicial Academy	Strategic goal failure	H	Development of precise action plan. Predefined communication channels. Regular meetings.
Missing projected deadlines due to ineffective procurement process	Strategic goal failure	H	Avoiding procurements under provisions of Serbian Law on public procurement

F.12.4. INVESTIGATE POSSIBILITIES E-LEARNING FOR THE MOST COMMON TRAININGS

Preconditions of Strategic Action

- Readiness of the Judicial Academy to lead the process of implementation of e-learning in the justice sector
- Supportive infrastructure (e.g. large enough bandwidth)

Major steps of the Strategic Action

1. Establish a working group, arrange the brainstorming workshops to identify the training needs;
2. Start the **e-learning project**, secure the funding;
3. Define the training objectives, main topics, training methods, trainers (the content developers), technology to be used requirements to be implemented;
4. Estimate costs: implementation cost and other resources, operational costs (to organise);
5. Select and train internal (Judicial Academy) staff for e-learning framework usage, implementation and maintenance

6. **Tender** the development and implementation (with a focus on training of the above selected internal staff and basic implementation);
7. Develop, design and run the **pilot course** (including the training materials);
8. Evaluate the results, make decisions about possible implementation e-learning for the whole sector, with wider selection of topics.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 20,000 and 100,000 EUR	Between 250 and 1000 man days	15 months

Even if open-source solution is used, the necessary knowledge to build an e-learning infrastructure and to develop training materials, might require significant third party resources, OR investment in own staff to learn how to use, implement and maintain such e-learning framework solutions. Therefore the material resources / internal human resources are interchangeable in this case. In determining the costs, we used the approach of utilizing internal resources as far as possible.

Consultants' recommended priority of the Strategic Action

This Strategic Action implicitly affects the whole Justice sector, although during pilot operations only a few trainings may be developed and evaluated. On the other hand it contributes to the high level ICT goals, like "Increase ICT proficiency of end-users...". Its combined effect is 3 on a scale of 1-4.

Although this activity is classified in the "forbidden zone" according to a survey, team of experts from Steering Committee together with the experts competent for the development of education in the Judicial Academy agreed that this action should be transferred to the category of "strategic investment". Start-up costs and initial resources should remain the same.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and funding or co-funding
Judicial Academy	Project management, pedagogical know-how, learning e-learning framework, developing e-learning pilot, training material, developing and operating e-learning framework, evaluating e-learning pilot.
ICT unit or organisation	Providing Content know-how and quality assurance of e-learning training materials

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Inappropriate technology, software or services selected for the pilot project	Insufficient level of functionality and reliability	M	Involvement of highly qualified specialists (pedagogical and content know-how) within the pilot
Missing project deadlines due to insufficient project involvement from the business (content) side	Strategic goal failure	H	Implementation of an efficient project management structure and management processes
Missing projected deadlines due to ineffective procurement process	Strategic goal failure	H	Avoiding procurements under provisions of Serbian Law on public procurement

F.12.5. ESTABLISH A DOCUMENTATION CENTRE WITHIN THE JUDICIAL ACADEMY

Preconditions of Strategic Action

- Take preparatory measures to structure and enable the Judicial Academy to take part in the creation of the Documentation Centre, and its later maintenance and updates; this includes additional human resources, systematization, space and other components of the new system.
- Involve the ICT unit or organisation, in the planning, design and implementation of the Documentation Centre and its linking to existing case law systems, across the sector.
- Ensure that appropriate standards are defined, before the start of creation of the documentation Centre, including data formats, meta-data standards, security rules, etc.
- Develop a proper advertising plan and scheme to explain the significance of such Documentation Centre to all future users, so that they would be ready and willing to start using it, as soon as available.

Major steps of the Strategic Action

1. Identify whether all preconditions have been met, in order to start the actions on establishment of the Centre;
2. Ensure that the Justice Sector management approves of the expanded functionality of the Judicial Academy, in order for it to take responsibility for the future maintenance and updates to the Centre database, with ICT organization taking care of the technical part of that, and providing IT links to relevant case management systems.
3. Define required hardware, software, network, power, backup, functional and security requirements;
4. Estimate costs, secure initial funding and sustainable budget for the future maintenance, perhaps through a phased approach, or in combination with another donor ICT-related project in the Justice Sector;
5. Once the funding is approved and the Judicial Academy expanded functionality is officially approved, ICT organization can take steps to initiate the procurement of the new system, with predefined Terms of Reference, describing both functional and technical conditions.
6. If the funding is provided through one of foreign donors, from a country with a successfully running similar Centre, then there could be a mapping of their existing Centre onto the one for Serbian Justice Sector, with necessary modifications to respect the differences between two systems. This approach was used in the case of Bosnia, where the Spanish government has donated funds as well as transfer of knowledge and products to equip the new centre in Sarajevo.
7. Tender the development and implementation of the new Documentation Centre, with ICT organization controlling the project management, and Judicial Academy serving in the role of functional advisor.
8. Select vendors and procure hardware, software and services;
9. Setup and implement JA Document Centre storage(s) and information portal.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 100.000 and 500,000 EUR	Between 250 and 1000 man days	5 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affect the whole Justice sector and contributes to some high level ICT goals like "Provide sector wide knowledge sharing and access to relevant information", "Improve functionality and coverage of ICT systems" and "Ensure uniform capability of ICT services, tools and methods across the sector". the combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Project management, system implementation, links to CMS
Judicial Academy	Functional specs, space, resources to maintain and update the system
Supreme Court of Cassation	Functional specs, space, resources to maintain and update the system
High Judicial Council, high Prosecutorial Council	Functional specs, space, resources to maintain and update the system

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of appropriate funding	Strategic goal failure	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Inappropriate technology, products or services selected	Insufficient level of functionality, reliability or performance	M	Involvement of highly qualified specialists in the development of technical specifications and evaluation of proposals.
Missing projected deadlines due to ineffective procurement process	Strategic goal failure	H	Avoiding procurements under provisions of Serbian Law on public procurement

F.12.6. DEVELOP A COMMONLY USED SET OF METADATA TO IDENTIFY CASES AND CASE RELATED DOCUMENTS

Preconditions of Strategic Action

- Assign a composite team of ICT and business area knowledgeable staff, to work on this task.
- Familiarize with the relevant and necessary standards used in the area of metadata definition.
- Setting up of a common data structure framework for a specified initial set of judiciary case-related documents and (if needed) web site(s).
- Through a series of well-designed workshops and publications for non-IT staff, publicize the need for creation of standard sets of metadata and raise interest for their application.

Major steps of the Strategic Action

1. Task team to identify all relevant information (data) that could qualify for metadata definition, for the selected courts' documents and data repository;
2. Define a commonly used set of metadata for each group of documents to be used, respecting the standards; at the same, time the team must establish clearly defined standards for the location, type and size of each data element subject to metadata definition on every case document to be used in this fashion, to ensure its proper use in the future.
3. These data standards for the selected case-related documents must then be applied to all such documents, regardless of the location of the court and its previous use of such documents.
4. Establish a common database containing all defined metadata sets for various document types, web sites, etc. related to key judicial processes.
5. Test the validity of selected metadata for each of the selected groups of case-related documents;
6. Make necessary corrections to the metadata definitions;
7. Familiarize all staff to be involved in the use of metadata about their structure, location, accessibility, etc.;

8. Setup and implement internally commonly accessible court documents standard formats and meta-data storage.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20,000 EUR	Between 250 and 1000 man days	3 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the Judicial branch of the Justice sector and contributes to some high level ICT goals like "Increase knowledge and proficiency", "Improve functionality and coverage of ICT systems" and "Ensure uniform capability of ICT services, tools and methods across the sector". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Forming of metadata composite team, management of the process, propagating the need for document standards
High Judicial Council	Participating in the Action, by directing courts on their necessary participation
Various courts	Participation in the composite team, through selected representatives

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of appropriate funding	Strategic goal failure	M	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Inappropriate process selected	Insufficient level of functionality, reliability or performance	M	Involvement of highly qualified specialists in the development of technical metadata specifications.
Low acceptance by the courts of the whole principle of metadata use	Failing attempt to use metadata, loss of common standards for case-related documents	M	Well-designed preparations and internal familiarization with the need for metadata and case-related documents common standards
Missing projected deadlines due to ineffective procurement process	Strategic goal failure	H	Implement good management practices, ensure high-level support for the Action (HJC support)

F.12.7. ESTABLISH A SEARCHABLE PORTAL FOR CASE LAW RELATED INFORMATION AND LEGAL DATABASE FOR THE GENERAL PUBLIC AND EXTERNAL LEGAL PROFESSIONALS

Preconditions of Strategic Action

- Establish a Documentation Centre within the Judicial Academy
- Develop a commonly used metadata to identify cases and case related documents

Major steps of the Strategic Action

1. Planning the scope of the system in terms of functionality and content. Involve professional legal bodies in specification.
2. Providing financial resources for development, maintenance and updating
3. Tendering and contracting of the system implementer
4. Monitoring of the system design and implementation
5. Develop interfaces to Documentation Centre
6. Develop processes which guarantee that only up-to-date information is accessible on the portal (plus historical information on previous versions of regulations)
7. Test, acceptance, training and deployment

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 100,000 and 500,000 EUR	between 250 and 1000 man days	4 quarters for initial realization

Consultants' recommended priority of the Strategic Action

This Strategic action affects mainly the Judicial branch of the Justice sector and contributes to some high level ICT goals like "Ensure widely available web-based services for all users", "Provide sector wide knowledge sharing and access to relevant information" and "Improve functionality and coverage of ICT systems". the combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Specification, Project management
Judicial Academy	Hosting the portal, participation in deployment, and operations
All judicial institutions	Specification, end-user testing

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of legal information	Delayed implementation	H	Timely provision of adequate legal information from all institutions included in the system
Large number of users	Difficult access	H	Planning the necessary technical resources for seamless access to a large number of users
Delayed content update	Lack / Loss of interest	H	Planning the human resources needed for timely update

F.12.8. IMPLEMENT KNOWLEDGE SHARING FUNCTIONALITY (MAILING LISTS, INTRANET PAGES, DISCUSSION FORUMS) WITHIN THE JUSTICE SECTOR

Preconditions of Strategic Action

- none

Major steps of the Strategic Action

1. Determine structure and tools of knowledge sharing by functional areas.
2. Identify the most suitable portal solution on the market
3. Acquire and implement the solution
4. Publish relevant documents
5. Develop internal processes which enable knowledge sharing.
6. Communicate and motivate the staff to use the knowledge sharing tools

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 20.000 and 100,000 EUR	Between 250 and 1000 man days	4 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to few high level ICT goals like "Increase knowledge and proficiency". The combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and funding
All justice sector institutions	Actively participate in the knowledge sharing
ICT unit or organisation	Project management, review of results

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
The knowledge sharing tools are not widely used	The institutional knowledge building at a reduced pace	M	The tools should always be updated with the latest relevant information and the staff properly motivated to use them.
Staff members will not feed the knowledge sharing tools with knowledge items/documents	There will not be real content, tool will not verify the investment.	H	Develop internal procedures and motivation for "feeding" the common knowledge base.

F.12.9. ASSESS ALL LOCALLY DEVELOPED APPLICATIONS AND SUPPORT THE ROLLOUT OF THE MOST USEFUL SYSTEMS

Preconditions of Strategic Action

- Get approval from the Ministry's management and individual institutions to have access to all necessary information regarding existing individual local applications

Major steps of the Strategic Action

1. Collection of all relevant information about the local applications, using reports from this project.

2. Perform analysis of features, technical requirements and functional specs for each application, using a standardized method for all.
3. Form a working group with reps from all key institutions in the sector, which would be used as the sounding board for the applicability of each local application elsewhere in the sector.
4. Create a report with the recommendations for use of local applications at certain institutions.
5. Discuss with each institution which would be a new user of any such application, the necessary conditions and possible required modifications, and implement them.
6. Develop (or improve) system documentations to meet standards and decrease dependence on vendors or individuals
7. Consider intellectual property rights and make necessary amendments for system-wide roll-out
8. Establish a rollout schedule, taking into account the real ability to deliver, install and test local applications at various other institutions over a period of time; define hardware, software, network, power, backup, functional and security requirements.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20,000 EUR	between 50 and 250 man days	4 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects mainly the Judiciary branch of the Justice sector and supports some high level ICT goals, like "Increase knowledge and proficiency" and "Ensure uniform capability of ICT services, tools and methods across the sector". The combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Project management, analysis, report creation, implementation
Various institutions in the sector	Contributing both local applications and information

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Inappropriate technology or institution selected	Insufficient level of functionality, reliability or performance to fit the selected institution	M	Involvement of qualified specialists ICT organization in the analysis of technical specifications and evaluation of applicability at various sites.

F.12.10. ESTABLISH KNOWLEDGE SHARING FUNCTIONALITY OF THE SERVICE DESK

Preconditions of Strategic Action

- Establishment of a professional Service Desk on sector level (which registers all ICT issues)

Major steps of the Strategic Action

1. Implementation of knowledge sharing functionality (mailing lists, Intranet pages, discussion forums) within the Justice Sector for selected organisation units
2. Regulate the operations of Service Desk staff to regularly review resolved ICT issues and register the experience in the knowledge base
3. Publish resolution of simplest ICT problems for end users to promote self-service

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 20,000 and 100,000 EUR	between 50 and 250 man days	1 quarter

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice Sector and contributes to some High level ICT goals, like: "Provide sector wide knowledge sharing and access to relevant information", Ensure supportive working environment and high system availability" and "Ensure uniform capability of ICT services, tools and methods across the sector"

Affected organisations and their role

Institution	Role
ICT unit or organisation	Specification knowledge sharing functionality. Coordinate development/implementation. Coordinate gathering most typical problems and their resolution
All judicial institutions	Contribution to the database by giving most typical problems and their resolution

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Knowledgebase will lack the most relevant cases at the beginning	ICT staff will not use the knowledgebase, because lack of useful information	H	Carefully planned gathering of the most common issues and their resolution during implementation.
ICT Staff members will not keep the ICT issues database up-to-date	Missing or not actual information, resulting in extra work with "reinventing the wheel" all the time a common problem is encountered	M	Management control over the improvement of the knowledge base Motivation of the highest contributors

F.12.11. ORGANISE ANNUAL ICT CONFERENCES WITHIN THE JUSTICE SECTOR

Preconditions of Strategic Action

- none

Major steps of the Strategic Action

1. Establish a working group, arrange the brainstorming session to identify the goal, topics, training methods, presenters/lecturers (internal and external), technology and visual training aids to be used, venue, timing and other related issues of the conference;
2. Invite the guest-lecturers;
3. Develop the agenda, handouts, feedback-lists, registration list;
4. Estimate operational costs;
5. Develop the presentations monitor the preparation of the presentation to assure the quality;
6. Handle logistic and other practical issues (incl. accommodation and catering), invitations to the participants and guests; translations and interpretations if necessary; printing if necessary; welcome-poster etc.
7. Evaluate the results

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20,000 EUR	Less than 50 man days	1 quarter

Consultants' recommended priority of the Strategic Action

This Strategic Action has effect on the whole Justice sector and contributes to a few high level ICT goals, like: "Improve ability to raise funds for ICT and to efficiently manage available funds", "Increase knowledge and proficiency". Its combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and funding or co-funding, invitation of external lecturers
Judicial Academy	Project management, pedagogical know-how about organising training events and principles of interactive training
ICT unit or organisation	Content know-how, assembly of conference programme

Major risks

The top risks for the implementation of the action are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Presentations turn into lecturing and one-way communication	Inefficient training event. Low quality of the event. The participants' expectations have not been realized	M	Monitoring of the preparation process by the training expert to assure the quality
Business decision makers not taking part	ICT remains internal issue for the ICT staff, business feedback is not gathered	H	Obtain high level support from the Ministry

F.13. ENSURE WIDELY AVAILABLE WEB-BASED SERVICES FOR ALL USERS

F.13.1. SETTING UP A COMMON DATA STRUCTURE FRAMEWORK FOR COURT INFORMATION PUBLICATION

Preconditions for the Strategic Action

- none

Major steps of the Strategic Action

1. Identify experts in all types of courts to participate in the development of common data framework
2. Identify internal IT experts who will lead technical development and form a working group
3. Circulate draft framework for comments and feedback to all stakeholders and independent experts

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20.000 EUR	Between 50 man days and 250 man days	2 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects one crucial branch of the Justice sector and supports the realisation of some strategic goals, like "providing web-based access to general public", or "have uniform ICT services and tools". The estimated combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Project management, specification of framework
Selected courts that will provide experts for the working group	Providing information and feedback on draft framework

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of cooperation from courts	Incomplete and/or vague common data specification	M	Communicate the importance of cooperation to all courts involved
Poorly defined specification	Difficulties and duplication of effort during implementation of court automation systems and integration with central court information portal.	M	Ensure participation of qualified IT and database specialists in the working group.

F.13.2. SET UP A CENTRAL LOCATION FOR PUBLIC COURT DOCUMENT STORAGE AND ACCESS

Preconditions of Strategic Action

- Setting up a common data structure framework for court information publication
- Develop a proper authentication and authorisation scheme for accessing published documents on court portal

Major steps of the Strategic Action

1. Identify physical location(s) for the court documents and data repository;
2. Define hardware, software, network, power, backup, functional and security requirements;
3. Estimate costs, secure initial funding and sustainable budget for the future maintenance;
4. Tender the development and implementation
5. Select vendors and procure hardware, software and services;
6. Setup and implement court document storage(s) and court information portal;
7. Define and implement document gathering procedures, upload and classify initial documents

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 100.000 and 500,000 EUR	Between 250 and 1000 man days	4-6 quarters

Consultants' recommended priority of the Strategic Action

This Strategic Action affects the judicial branch of the Justice sector, but other branches may profit from it by accessing information and contributes to several high level ICT goals. The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Requirement specification, Tendering, Project management
Judicial institutions	Contribute to requirement specification, prepare court documents for upload

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Inappropriate technology, products or services selected	Insufficient level of functionality, reliability or performance	M	Involvement of highly qualified specialists in the development of technical specifications and evaluation of proposals.
Missing projected deadlines due to ineffective procurement process	Strategic goal failure	H	Avoiding procurements under provisions of Serbian Law on public procurement

F.13.3. DEVELOP A PROPER AUTHENTICATION AND AUTHORIZATION SCHEME FOR ACCESSING PUBLISHED DOCUMENTS ON COURT PORTAL

Preconditions of Strategic Action

- Setting up a common data structure framework for court information publication

Major steps of the Strategic Action

1. Establish a working group and arrange the workshops to domains and user groups for accessing court portal and other applications;
2. Determine the types of court documents which might be accessible at the court portal and determine which documents may be published without access restrictions and which are restricted. Define the "roles" of possible actors accessing these documents (advocates, prosecutors, witnesses, parties of a case, etc.)
3. Define the procedures for registration, and authorisation and modify relevant laws to allow access of certain court documents. Involve the Chamber of Advocacy and other professional organisations.
4. Define the architecture and decide about eventual inter-site and intra-site replication nodes, for increased availability and reliability of the central (external) user repository;
5. Define hardware and software requirements
6. Secure funding
7. Procure and configure the external user directory
8. Link the external user directory to the authentication system of the Court portal and adjust the Court portal to enable download of the specific documents after proper authorisation.
9. Modify/develop automatic interfaces between the Case Management systems and the Court portal to publish the accessible documents
10. Train the users of the Case Management systems about the modified processes and functions of the CMS systems.
11. Communicate the changes of the Court portal for involved advocates and other parties

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 100.000 and 500,000 EUR	Between 250 and 1000 man days	6 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects one crucial branch of the Justice sector and supports the realization of some strategic goals, like providing web-based access to general public, or having uniform ICT services and tools. It is also a precondition to implementation of performance measurements. The estimated combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Project management, technical lead
Courts	Participation in specification of accessible documents and later in trainings

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of appropriate funding	Strategic goal failure	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Legal changes regulations will not be enacted within proper time	Late implementation	H	Proper preparation, phased implementation, involvement of all interested parties in preparations
Inappropriate technology, products or services selected	Insufficient level of functionality, reliability or performance	M	Involvement of highly qualified specialists in the development of technical specifications and evaluation of proposals.
Missing projected deadlines due to ineffective procurement process	Strategic goal failure	M	Assigning qualified and experienced project managers in the ICT unit or organisation to lead the effort;

F.13.4. DEVELOP A COMMON FORM MANAGEMENT COMPONENT TO COVER ALL FORMS TO-BE IN ELECTRONIC FORMAT

Preconditions of Strategic Action

- none

Major steps of the Strategic Action

1. Establish a working group comprised of IT experts, graphics designers and representatives from all types of courts.
2. Arrange the series of workshops to select best existing paper forms that will be used as a model for digitalization;
3. Identify opportunities for merging or discontinuing some of the existing forms, in order to minimize the number of different forms in use (may changes of the business processes and changes in the legal framework);
4. Procure software component for electronic forms management
5. Assign responsibilities and develop electronic templates for the remaining forms
6. Implement pilot-testing for selected and most frequently used electronic forms

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20.000 EUR	Between 50 man days and 250 man days	3 quarters

Implementation (or modification) of applications receiving these forms electronically is carried out by separate strategic actions, thus the direct investments of these actions are relatively low.

Consultants' recommended priority of the Strategic Action

This Strategic action affects entire court system and is a precondition for the realization of all strategic goals related do electronic document management, electronic forms submission and public web access to court documents. The estimated combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding, initiation of necessary lgal changes

Institution	Role
ICT unit or organisation	Project management Selection and Implementation of form management application Coordination of form design and mapping of existing forms
All courts	Consulting, providing existing forms used in their courts

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of cooperation from courts	Incomplete set of electronic forms	M	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Software component for forms management that is difficult to use	Inefficient and cumbersome forms management	M	Involvement of highly qualified specialists in the development of technical specifications and evaluation of proposals.
Lack of qualified specialists assigned to manage electronic forms.	Insufficient level of functionality	M	Involvement of highly qualified specialists in the development of technical specifications and evaluation of proposals.
Missing projected deadlines due to ineffective procurement process	Strategic goal failure	H	Avoiding procurements under provisions of Serbian Law on public procurement

F.13.5. ENABLE ELECTRONIC FORM SUBMISSION FOR CITIZEN'S INQUIRIES

Preconditions of Strategic Action

- Setting up a common data structure framework for court information publication
- Set up a central location for public court document storage and access
- Develop a proper authentication and authorization scheme for accessing published documents on the court portal
- Develop a common form management component to cover all forms-to-be in electronic format

Major steps of the Strategic Action

1. Conduct feasibility study and verify that legal framework allows for electronic forms submission.
2. Get support and approval to implement electronic submission of selected inquiries for citizens (e.g. request for legal status certificate).
3. Define the procedures and policies for electronic forms submission via court portal and handling the e-filed documents and payments;
4. Investigate needs for regulatory changes, and initiate required laws, bylaws or other regulations.
5. Implement new procedures for handling electronic form submission of selected citizen inquiries in selected pilot courts (e.g. Belgrade)
6. Monitor pilot-implementation and perform changes if necessary.
7. Phased training and implementation of the e-filing in more courts

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20.000 EUR for the basic forms	Between 50 and 250 man days	4 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action requires relatively small investment and can provide quick wins and public attention (visibility). It affects mainly the judicial branch of the Justice sector and contributes to some high level ICT goals like "Ensure widely available web-based services for all users", "Ensure uniform capability of ICT services, tools and methods across the sector" and "Improve functionality and coverage of ICT systems". The estimated combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding, initiation of necessary legal changes
ICT unit or organisation	Project management
Selected courts	Participation in pilot e-filing program

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Obstacles in the legal framework	Inability to implement strategic action	H	Enacting changes in the laws and court rules of procedure, to support e-filing and electronic document management.
Lack of qualified specialists assigned to manage electronic forms.	Insufficient level of functionality	M	Involvement of highly qualified specialists in the development of technical specifications and evaluation of proposals.
Low usage rate of electronic form submission at the court portal	Questionable value of investment	M	Organize awareness campaigns in media

F.13.6. ENABLE ELECTRONIC FORM SUBMISSIONS FOR LEGAL PROFESSIONALS FOR SELECTED PROCESSES

Preconditions of Strategic Action

- Setting up a common data structure framework for court information publication
- Set up a central location for public court document storage and access
- Develop a proper authentication and authorization scheme for accessing published documents on the court portal
- Develop a common form management component to cover all forms-to-be in electronic format

Major steps of the Strategic Action

1. Conduct feasibility study and verify that legal framework allows for electronic forms submission;
2. Get support and approval to implement electronic forms submission for legal professionals;
3. Define the procedures and policies for electronic forms submission;
4. Define the procedures and policies for handling and processing of e-filed documents in the courts;
5. Investigate regulatory needs and initiate amendments to laws, bylaws and other regulations if necessary.
6. Implement support for electronic forms submission on the central court portal.
7. Implement distribution of received electronic forms to relevant internal organisational units
8. Assign an administrator for managing the accounts for users and firms/agencies.
9. Create accounts and organize training for several pilot users (e.g. legal offices).

10. Monitor pilot-implementation, gather feedback and perform changes if necessary.
11. Create written and video tutorials for e-filing and raise awareness of the new functionality
12. Train court users and implement support for e-filing in all case management systems

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 20.000 and 100,000 EUR	Between 250 and 1000 man days	4 quarters

Consultants' recommended priority of the Strategic Action

Allowing electronic forms submission to wide range of legal professionals is "game changer" feature and important strategic step towards the e-Justice. This Strategic action has effect on mainly the judiciary branch (but prosecutorial and penitentiary processes can also be facilitated) and contributes to some high level ICT goals like, "Ensure widely available web-based services for all users", "Ensure uniform capability of ICT services, tools and methods across the sector" and "Improve functionality and coverage of ICT systems". The estimated combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding, facilitating changes in legal framework
ICT unit or organisation	Project management
Legal professionals (e.g. represented by Chambers) and external organizations (e.g. Police)	Participation in specification and pilot e-filing program

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Obstacles in the legal framework	Inability to implement strategic action	H	Enacting changes in the laws and court rules of procedure, to support e-filing and electronic document management.
Lack of qualified specialists assigned to manage electronic forms.	Insufficient level of functionality	M	Involvement of highly qualified specialists in the development of technical specifications and evaluation of proposals.
Low usage rate of electronic form submission at the court portal	Questionable value of investment	M	Organize awareness campaigns in media

F.13.7. IMPLEMENT PERSONALISATION AND NOTIFICATION OF REGISTERED USERS AT CENTRALISED COURT PORTAL

Preconditions of Strategic Action

- Setting up a common data structure framework for court information publication.
- Set up a central location for public court document storage and access.
- Develop a proper authentication and authorization scheme for accessing published documents on the court portal.
- Develop common look-and-feel standards for all web pages of the sector.

- Consider all necessary legal changes required to implement proposed new ICT delivery channels in Justice Sector.
- Define technical standards for the implementation of new ICT delivery channels.
- Procure, develop and implement additional software elements/systems necessary to utilize the new ICT delivery channels.
- Include the additional delivery channels into common IT security methodology and procedures.

Major steps of the Strategic Action

1. Conduct feasibility study and verify that legal framework is ready for new delivery channels;
2. Define the procedures and policies for electronic notifications and billing;
3. Arrange VAS service level agreements with mobile providers (or with VAS brokers);
4. Implement support for personalization and electronic notifications on the central court portal and/or individual court portals.
5. Create written and video tutorials for electronic notifications and raise public awareness.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20,000 EUR	Between 250 and 1000 man days	2 quarters

Consultants' recommended priority of the Strategic Action

This strategic action frees court personnel from responding to daily inquiries on case status, and enables legal professionals to obtain required information with minimal effort. In addition, it can provide additional sources of income for the judiciary budget. The Strategic action affects the judiciary branch of the Justice sector and contributes to some high level ICT goals like, "Ensure widely available web-based services for all users" and "Improve functionality and coverage of ICT systems". The estimated combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Project management
Selected courts	Participation in defining notification procedures and policies.

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Obstacles in the legal framework	Inability to implement strategic action	H	Enacting changes in the laws and court rules of procedure, to support new information delivery channels.
Low usage rate of webpage personalization and electronic notification system	Questionable value of investment	M	Organize awareness campaigns in media

F.13.8. PROVIDE CAPABILITY FOR PAYMENT OF COURT TAXES AND FEES TO CITIZENS AND LEGAL PERSONS

Preconditions of Strategic Action

- Define common master data used for all systems.
- Consider all necessary legal changes required to implement proposed new ICT delivery channels in Justice Sector.
- Define technical standards for the implementation of new ICT delivery channels.
- Procure, develop and implement additional software elements/systems necessary to utilize the new ICT delivery channels.
- Include the additional delivery channels into common IT security methodology and procedures.

Major steps of the Strategic Action

1. Conduct feasibility study and verify that legal framework is ready for new delivery channels;
2. Check the governmental intentions (e-Government strategy) and plans to implement an electronic payment system for the public administration and align court payment implementation with them if feasible.
3. Define the procedures and policies for electronic notifications and billing;
4. Arrange data exchange agreements and protocols with Ministry of Finance / Treasury department;
5. Implement automated payment tracking in the existing and future court information systems
6. Install payment terminals

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 20.000 and 100,000 EUR	Between 250 and 1000 man days	4 quarters

*) The above cost estimation is valid only if Justice sector can join the e-Government payment infrastructure and the terminals are financed by banks in return for share of commission (PPP construction).

Consultants' recommended priority of the Strategic Action

This strategic action will significantly improve financial aspect of the court business processes, and at the same time enables to court users easier fulfillment of their financial obligations, since they would not be required to physically deliver proofs of payments to the court. It affects the judicial branch and contributes to few high level ICT goals, like "Ensure widely available web-based services for all users", "Maintain various delivery channels while stimulating use of modern ICT communication tools" and "Improve functionality and coverage of ICT systems". The estimated combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Project management
Treasury department	Exposing web services for daily collection of XML statements
Affected courts	Active use of the system, providing feedback for improvements

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Obstacles in the legal framework	Inability to implement strategic action	H	Enacting changes in the laws and court rules of procedure, to support electronic payment processing.
Low usage rate of electronic payment	Questionable value of investment	M	Organize awareness campaigns in media
Overlaps or gaps with governmental level e-payment implementation	No support from central government, delayed implementation, not implemented legal regulations	H	Form a working group with governmental institutions responsible for e-government implementation and develop a common agenda and technology white paper.

F.13.9. DEVELOP NEW PORTAL FOR JUDICIAL ACADEMY WHICH ENABLES AUTOMATIC PUBLICATION OF TRAINING CALENDAR, TRAININGS COURSES AND TRAINING MATERIALS

Preconditions of Strategic Action

- Implement a comprehensive Training Register to support the whole training process

Major steps of the Strategic Action

1. Specify requirements toward the JA portal (together with interface requirements)
2. Acquire and implement the solution
3. Define portal update responsibilities (for not automated contents) and train Judicial Academy staff
4. Regularly update the contents on the portal and advertise the portal and its benefits within the Justice sector

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20,000 EUR	Between 50 man days and 250 man days	1 quarter

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole justice sector and contributes to a few high level goals like "Develop new portal for Judicial Academy which enables automatic publication of training calendar/ trainings courses / training materials" and "Increase ICT proficiency of end users, ICT staff and decision makers through training".

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and funding
Judicial Academy	Specify and maintain the portal on regular basis
ICT unit or organisation	Project management, review of results

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
The portal is not widely used	The information dissemination and communication levels within the sector have reduced effect	M	The portal should always be updated with the latest relevant information and advertised on all training events of the JA.

F.14. MAINTAIN VARIOUS DELIVERY CHANNELS AND STIMULATE USAGE OF MODERN ICT RESOURCES

F.14.1. CONSIDER ALL NECESSARY LEGAL CHANGES REQUIRED TO IMPLEMENT PROPOSED NEW ICT DELIVERY CHANNELS IN JUSTICE SECTOR

Preconditions of Strategic Action

- Establishment of a working group/committee, made up of both legal and ICT technical experts, to consider all new possibilities for information-exchange channels in the justice sector, influence of EU rules and practices

Major steps of the Strategic Action

- Set up the new legal/technical working group at the sectorial level to consider new/alternative information-exchange channels of communication
- Consider wider, government-wide changes in the area of communication channels to citizens and clients for government services
- Organize visits, familiarization with all key organizations and well-applied legal conditions for new ICT channels within justice sectors across Europe;
- Review current and upcoming legal regulations that could affect and/or contribute to expansion of communication channels for government services clients, with special view of justice sector;
- Consider all technical and infrastructure current and future conditions for implementation of the new communication channels in the justice sector;
- Consult with political & governmental institutions to gather support and momentum for the modernization of information exchange between government and citizens/clients, with special view of the justice sector needs
- Based on the above, write a report with the findings and recommendations;
- Ensure the support from both Serbian government and EU institutions to implement the most lucrative/efficient solutions, as recommended in the report

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20,000 EUR	Between 50 and 250 man days	2 quarters

Human resource estimations considered approx. working group with up to 10 members, 15 meetings, some travel/visits, documents writing/translation

Consultants' recommended priority of the Strategic Action

This Strategic Action affects the whole Justice sector and supports a few high level ICT goals, like: "Maintain various delivery channels...", "Improve functionality and coverage of ICT systems". The combined effect is 2 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Project management
Other government institutions in charge of communication channels	Political and legal support and opinion
EU institutions, including pan-European legal organizations and EU Delegation to Serbia	Political, technical and organizational support, knowledge and standards exchange

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of appropriate top-level political support	Strategic goal failure	H	Proactive seeking for political support, searching for top-level political sponsor, both within the Serbian government and EU
Inability of the working group to perform effectively, getting in sync legal and technical pre-conditions	Insufficient level of knowledge, professional capacity or interest in the problem	M	Involvement of highly qualified & interested specialists in the work; finding innovative ways to gather their interest and active support.

F.14.2. DEFINE TECHNICAL STANDARDS FOR THE IMPLEMENTATION OF NEW ICT DELIVERY CHANNELS

Preconditions of Strategic Action

- Establishment of the ICT unit or organisation; this organization would be an obvious candidate to establish such technical standards, along with all other applicable ICT standards in the sector.

Major steps of the Strategic Action

- Get internal/sectorial support to initiate work on the new standards;
- Establish links/relationships with other relevant standards institutions, both in Serbia and EU;
- Organize visits, familiarization with all key organizations and well-applied standards justice sectors across Europe;
- Identify all relevant, recommended and applicable new ICT delivery channels;
- Investigate wider technical background and applicable standards, both within Serbia and EU;
- Define hardware, software, network, power, backup, functional and security requirements for such new ICT delivery channels, specifically applicable within the justice sector;
- Define required specific standards for each adopted new ICT channel, as extension of existing national/EU standards, if necessary, otherwise just define which already existing standards apply;
- Promote these standards across the sector, and propagate their value to top management;
- Include the above standards specifications in any future projects related to these new ICT channels.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20,000 EUR	Between 250 and 1000man days	4 quarters

Consultants' recommended priority of the Strategic Action

This Strategic Action affects the whole Justice sector and contributes to a few high level ICT goals, like: "Maintain various delivery channels...", "Ensure uniform capability of ICT services, tools and methods.". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Definition of standards

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of appropriate political support	Strategic goal failure	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Lack of funding	Some new channels introduced without adherence to proper standards	M	Involvement of highly qualified specialists in the development of standards, get support, funding from donors

F.14.3. PROCURE, DEVELOP AND IMPLEMENT ADDITIONAL SOFTWARE ELEMENTS/SYSTEMS NECESSARY TO UTILIZE THE NEW ICT DELIVERY CHANNELS

Preconditions of Strategic Action

- Establishment of all necessary legal pre-conditions and technical standards required for the successful implementation of a new ICT service, through procurement/design of additional software elements/systems.
- Wider, sector-wide establishment of a need for such new ICT channel in a particular institution, or group of institutions (e.g. all Misdemeanour Courts).

Major steps of the Strategic Action

1. Identify the actual business requirements for such new ICT channel, in cooperation with the potential user institutions;
2. Provide sufficient top management support for the introduction of the new software/system;
3. Based on the business requirements, create technical requirements for the new software/system, including Terms of Reference, with defined hardware, software, network, power, backup, functional and security requirements;
4. Estimate costs, secure initial funding and sustainable budget for the future maintenance;
5. Provide proper funding, either internally, or through a donor support;

6. Tender the development and implementation;
7. Select vendors and procure hardware, software and services;
8. Setup and implement the new software element/system.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 100.000 and 500,000 EUR	Between 250 and 1000 man days	5 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to a few high level ICT goals like "Maintain various delivery channels while stimulating use of modern ICT communication tools" and "Ensure uniform capability of ICT services, tools and methods.". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Project management, implementation
Various justice sector institutions, with interest in applying new ICT channel	Supply of business requirements, functional specs

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of appropriate funding	Strategic goal failure	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Inappropriate technology, products or services selected	Insufficient level of functionality, reliability or performance	M	Involvement of highly qualified specialists in the development of technical specifications and evaluation of proposals.
Missing projected deadlines due to ineffective procurement process	Strategic goal failure	H	Precise specification of requirements and evaluation criteria

F.14.4. INVESTIGATE MOST COST-EFFECTIVE APPROACHES AND TECHNOLOGIES FOR THE USE IN JUSTICE SECTOR

Preconditions of Strategic Action

- Establishment of all necessary legal pre-conditions and technical standards required for the successful implementation of a new ICT service channel, through procurement/design of additional software elements/systems.
- Establishment of the business needs for new ICT channels of communication, in a particular institution, or group of institutions (e.g. all Misdemeanour Courts), and subsequent use of the Effect/Effort prioritization chart, to establish the position of each new ICT channel within the four quadrants, in order to prioritize them.

Major steps of the Strategic Action

1. ICT body to investigate the possible approaches and technology alternatives for each of the top-priority ICT channels, as established earlier in the process, it may be necessary for that purpose to liaise with relevant external organizations in charge of the general use of additional delivery channels (e.g. mobile phones service providers, Internet service providers, etc.)
2. As the result, a collection of most cost-effective approaches and technologies per each priority new ICT channel should be created, for the use in Justice Sector, in a form of a report;
3. The report should be approved first by the legal/technical working group at the sectorial level and then by the relevant management, in order to proceed with the new ICT channels implementation;
4. Once the final decisions have been made on the sequence of implementation of the new ICT channels, adequate and timely public information and communication campaign should be organized, making it well-understood and accepted by any and all potential future users.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 20,000 and 100,000 EUR	Between 50 and 250 man days	2 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to a few high level ICT goals like "Maintain various delivery channels while stimulating use of modern ICT communication tools" and "Improve functionality and coverage of ICT systems". The combined effect is 3 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Project management, priority analysis, report writing
legal/technical working group at the sectorial level	Review of report, approval

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of appropriate funding	Strategic goal failure	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors)
Inappropriate approaches and technologies selected	Insufficient level of functionality, reliability or performance	M	Involvement of highly qualified ICT and business specialists.

F.14.5. INCLUDE THE USE OF ADDITIONAL DELIVERY CHANNELS INTO COMMON IT SECURITY METHODOLOGY AND PROCEDURES

Preconditions of Strategic Action

- Decision on the priority of implementation of some of the new ICT channels and their relevant technologies;

Major steps of the Strategic Action

1. Identify which ICT channels, considering their defined priorities, are the clear candidates to be integrated into the common IT security policy and procedures;
2. For each such channel, establish the necessary conditions under which such channel can operate and perform required functionality within the justice sector, while satisfying the security rules as required by the common IT security policy;
3. Define hardware, software, network, power, and other specific security requirements for each new ICT channel;
4. Consider the necessary potential changes that may have to be made to existing IT security policy and procedures, in order to integrate the new ICT channel, document and implement;

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 20,000 and 100,000 EUR, depending on selection and number of new ICT channels	between 250 and 1000 man days, depending on selection and number of new ICT channels	5 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to some high level ICT goals like "Maintain various delivery channels while stimulating use of modern ICT communication tools", "Improve functionality and coverage of ICT systems" and "Enhance Information Security". The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Providing approvals and co-funding
ICT unit or organisation	Project management, study of new requirements, definition of IT security policy changes

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of appropriate funding	Strategic goal failure	H	Proactive seeking for sources of funding (state budget, IPA project funds, donors), together with the funding for actual implementation of new ICT channels themselves
Inappropriate technology, products or services selected for a particular ICT channel	Incompatible security requirements of the new services with the sector common IT policy	M	Involvement of highly qualified specialists in the analysis and definition of new security requirements.
Missing projected deadlines due to ineffective process	Strategic goal failure	H	Avoiding procurements under provisions of Serbian Law on public procurement

F.15. ENSURE VENDOR-INDEPENDENT SERVICE ARCHITECTURE

F.15.1. INTRODUCTION OF BUSINESS PROCESS MANAGEMENT IN COOPERATION WITH THE BUSINESS AREAS

Preconditions of Strategic Action

- none

Major steps of the Strategic Action

1. Understand details and appropriateness of the Business Process Management. Create an effective BPM Implementation strategy.
2. Determine the costs and benefits of BPM implementation. Decide whether to proceed with an implementation and which path to take.
3. Evaluate the desirability of organizational processes for a BPM implementation. Prioritize processes for BPM project.
4. Decide which level of BPM maturity to follow. Develop the optimal roadmap for BPM adoption.
5. Implement BPM.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR*	between 50 man days and 250 man days	3 quarters

*) If a BPM tool is implemented, then it may have additional costs which depend on the package and the number of users. Simple tools allowing process modelling and documentation may be close to free.

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector and contributes to some high level ICT goals, like: "Align Business processes and ICT system functions through resilient and vendor independent ICT architecture", "Ensure uniform capability of ICT services, tools and methods across the sector" and "Ensure ICT systems sustainability". The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Preparing and implementing BPM
All institutions	Implementing BPM

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Business stakeholders are not involved in the BPM introduction on appropriate level	Strategic action failure	M	Business stakeholders should be trained/educated for BPM, including benefits of having processes described. BPM should be presented as process-based, not technology focused. Business stakeholders should be engaged from the start.

Risk analysis		Risk mitigation	
The organisation is not suited for BPM	Strategic action failure	H	Create stable foundation before start of the BPM initiative. Assess the maturity of people, processes and technology.

F.15.2. INTRODUCTION OF SERVICE ORIENTED ARCHITECTURE TO ENABLE FLEXIBILITY AND REUSABILITY

Preconditions of Strategic Action

- Implement Business Process Management
- Define common master data used for all systems
- Define message structure

Major steps of the Strategic Action

1. Develop SOA Strategy. Identify high-value processes that should be converted into business services. Obtain organisational buy-in and build standardized and formal SOA blueprint.
2. Assess the organisational readiness for SOA adoption. Assess people, processes and technology for SOA readiness and realize areas for improvement. Based on the readiness, decide on the model of SOA adoption:
 - Minimalist. Adopt by default as vendors shift products to SOA, but not take proactive steps.
 - Integration focused. Use services for easy integration of internal systems (most common approach, with limited business benefit).
 - Externally focused. Identify external system interfaces used by business partners and offer those as web services (value depends on adoption by other parties).
 - Radical. Seek out opportunities to exploit SOA and services.
3. Create SOA service catalogue.
4. Determine appropriate level of service granularity. Develop scalable and reusable services.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
More than 500,000 EUR	between 250 and 1000 man days	8 quarters

Consultants' recommended priority of the Strategic Action

This strategic action could have impact on the whole sector, if implemented appropriately. The justice sector should focus either on integration-focused or externally-focused SOA adoption strategies. The action contributes to some high level ICT goals, like "Align Business processes and ICT system functions through resilient and vendor independent ICT architecture", "Ensure supportive working environment and high system availability" and "Improve functionality and coverage of ICT systems". The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Introduce SOA

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
The Justice sector plans for a SOA "big-bang" approach	Strategic goal failure	M	Use a series of smaller projects when implementing and adopting SOA.
Justice sector implements vendor proprietary service	Loss of interoperability and flexibility benefits of SOA	M	Avoid vendor proprietary services, seek for open standards

F.15.3. ESTABLISH SECTOR-WIDE ARCHITECTURE MANAGEMENT RESPONSIBILITIES TO MAINTAIN A REGISTER FOR ICT SYSTEMS

Preconditions of Strategic Action

- Establishment of a central ICT unit or organisation, to fully manage all ICT-related sectorial business, technical and human resources issues

Major steps of the Strategic Action

1. Creation of regulations concerning the procedures for the creation, implementation and decommissioning of IT systems in the judiciary
2. Define attributes to be gathered for the individual ICT systems and establish a central database
3. Collection of detailed information on existing IT systems in the judiciary.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
less than 20,000 EUR	between 50 man days and 250 man days	2 quarters

Consultants' recommended priority of the Strategic Action

This Strategic Action affects the whole Justice sector and contributes to some high level ICT goals, like "Ensure uniform capabilities for ICT services, tools, ...", "Ensure ICT systems sustainability", "Enhance ICT security", "Align business processes and ICT system functions...". the combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Specification of data to be collected. Collection of detailed information, Development of change management procedures. Maintenance the register
All judicial institutions	Provision of information

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Lack of information from the judicial institutions	Incomplete register	M	Establishment of a central ICT organization, authorized to request and receive the information required from the judicial authorities
Inaccuracies in the future projects planning	Lack of provisioning of the same quality services to the clients of the Justice Sector	M	Establishment of a central ICT organization, authorized to manage all ICT-related sectorial business, technical and human resources issues Define and use change management procedures for ICT architecture

F.15.4. IMPLEMENT SOA ON THE NATIONAL E-GOVERNMENT INFRASTRUCTURE

Preconditions of Strategic Action

- Establishment of national e-Government infrastructure

Major steps of the Strategic Action

1. Investigation of available capacities and migration opportunities
2. Agree on service levels and conditions of infrastructure provision
3. Plan and develop required components of Service Oriented Architecture

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Between 20,000 and 100,000 EUR	Between 50 and 250 man days	6 months

Consultants' recommended priority of the Strategic Action

This Strategic Action affects the whole Justice sector and contributes to several high level ICT goals, like "Ensure uniform capabilities for ICT services, tools, ...", "Ensure ICT systems sustainability", "Enhance ICT security", "Ensure high availability and reliability". The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Provision of funding. Project definition and management

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
National e-Government infrastructure will not have the sufficient capacity for e-Justice	Low performance	M	Careful capacity planning and scheduling

F.16. ENSURE VENDOR-INDEPENDENT COMMUNICATION ARCHITECTURE

F.16.1. DEVELOP NETWORKS WITH SUFFICIENT CAPACITY

Preconditions for the Strategic Action

- Primary data centre needs to be in production

Major steps of the Strategic Action

1. Determine capacity needs considering the current requirements and the extrapolated needs for the next 5-6 years.
2. Prepare Feasibility Studies for outsourcing certain WAN/LAN services.
3. Tender vendors for the provision of WAN services – most preferably select one vendor for the whole WAN
4. Tender vendors for the LANs of the various institutions – there might be separate vendors for the various sites
5. Necessary software and hardware needs to be procured if equipment remains in the property of the justice institutions

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
more than 500,000 EUR*	between 250 and 1000 man days	8 quarters

*) Purchase of network capacities not only requires initial investments, but the yearly costs may form a significant part of the whole ICT budget, therefore it is critical to calculate the expected TCOs for various network components/services

Consultants' recommended priority of the Strategic Action

This strategic action affects the whole Justice sector and contributes to several high level ICT goals, like “Ensure supportive working environment and high system availability”, “Have a good balance of internal and external services having efficiency in mind”, “Enhance Information Security” and “Ensure widely available web-based services for all users”. The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Needs to provide adequate funding. Supervision of the project implementation
The ICT unit or organisation	Procures necessary hardware + networking + power equipment and data telecommunications services: Project management and implementation

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Telecommunications service provider does not provide adequate service	Loss of service	M	The telecommunication service provider chosen for WAN should satisfy following: <ul style="list-style-type: none"> • Has to have national wide redundant network, • Has to have enough technical and human resources to provide telecommunication service, • Has to have enough financial resources, • Has to be able to provide alternative backup lines for list mile connection (e.g. wireless or redundant physical connection),
Inadequate budget provision	Loss of service	M	Budgeting has to cover all direct and indirect costs and should be done on yearly level. Budgeting should come from the Serbian budget and/or donors' funding

F.17. ENSURE VENDOR-INDEPENDENT INTEROPERABILITY AND INFORMATION EXCHANGE ARCHITECTURE

F.17.1. DEVELOPMENT AND IMPLEMENTATION OF INTEROPERABILITY STANDARDS

Preconditions of Strategic Action

- none

Major steps of the Strategic Action

1. Develop message exchange standards for trusted exchange of information between stakeholders in the Justice sector.
2. Ensure Interoperable IT architecture, Implement interoperability standards on pilot institutions.
3. Assess implications on the legislation related to the Justice sector.
4. Implement interoperability standards.
5. Raise awareness about interoperability, communicate activities. Share best practices with other institutions. Monitor and evaluate, provide Interoperability governance.

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 20,000 and 100,000 EUR	between 250 and 1000 man days	4 quarters

Consultants' recommended priority of the Strategic Action

This strategic activity has significant impact over the whole sector. It contributes to some high level strategic goals like "Align Business processes and ICT system functions through resilient and vendor independent ICT architecture", "Ensure supportive working environment and high system availability" and "Improve functionality and coverage of ICT systems". The combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
ICT unit or organisation	Develop and implement interoperability standards

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
No political will to introduce interoperability standards	Strategic goal failure	M	Ensure top management of different institutions is informed and aware of the benefits of information exchange between the institutions.
Interoperability is implemented only on technical level	Lack of full benefit from the introduction of interoperability	M	Memorandum of understanding signed between involved institutions Legal, business experts involved in the development of legal, organisational and semantic interoperability levels

F.18. GOOD BALANCE OF INTERNAL AND EXTERNAL SERVICES WITH EFFICIENCY IN MIND

F.18.1. PREPARE FEASIBILITY STUDIES FOR OUTSOURCING OF VARIOUS ACTIVITIES

Preconditions of Strategic Action

- Prepare and implement long-term Feasibility Study and TCO methodologies

Major steps of the Strategic Action

1. Determining which activities will be subject to feasibility study (e.g. printer maintenance, workstation maintenance, network operations, data centre operations, etc.)
2. Define a uniform structure for outsourcing related Feasibility Studies
3. Decision of the way of feasibility study realization (own resources, external services), provide funds and resources, select and contract vendor if Feasibility Study is done by external party.
4. Gather detailed information on current costs, resource needs, quality parameters of the subject to be investigated
5. Prepare or assist in preparation of Feasibility Study
6. Acceptance of the outcome of the Feasibility Study

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
Less than 20kEUR	less than 50 man days per each feasibility study	1 quarter per each feasibility study Altogether 4 studies parallel in 2 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action affects the whole Justice sector since the outsourcing areas are usually services for most end-users. Feasibility studies support multiple strategic goals from increasing efficiency to ensure supportive end-user environment. The estimated combined effect is 4 on a scale of 1-4.

Affected organisations and their role

Institution	Role
MoJPA	Specification, Project management
Selected involved institutions	Data provision on current resource needs of service and user expectations

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Wide range of the feasibility study	Low impact when planning the necessary funds and technical parameters	M	Refining and specify areas that will affect the feasibility study
Long period between the feasibility study and implementation of outsourcing service	Changes in financial conditions for the realization of the outsourcing service Structural changes in the institutions that will benefit outsourcing services	H	Careful preparations for decision making

F.18.2. DEVELOP A DASHBOARD FOR IT SERVICE LEVEL MEASUREMENTS

Preconditions of Strategic Action

- Assembly of a service catalogue for all services provided by IT
- Establish a professional Service Desk on sector level with clear responsibilities of first line, second line and application support

Major steps of the Strategic Action

1. Define measurement methods for major service parameters
2. Development of dashboard for IT service level measurements
3. Regulate the data provision obligations (in case of manual feed for some measures)
4. Communicate the measurement results for the Ministry management

Resource and timing estimations

Material resources	Internal human resources	Implementation time needed
between 20,000 and 100,000 EUR	between 50 and 250 man days	3 quarters

Consultants' recommended priority of the Strategic Action

This Strategic action mainly affects the ICT organisation of the Justice sector and contributes to a few high level ICT goals like "Enhance ICT operations efficiency through performance measurement", "Have a good balance of internal and external services having efficiency in mind",

Affected organisations and their role

Institution	Role
ICT unit or organisation	Development of dashboard for IT service level measurements

Major risks

The top risks for the implementation of the program are the following:

Risk analysis		Risk mitigation	
Risk description	Effect of risk	Risk level (L/M/H)	Preventive actions
Data collection for defined ICT measures are hard to automate	Manual data feed is unreliable in most cases thus data will not be punctual or timely	H	Use simple measures which might be obtained from ICT systems (network, Service Desk). Use manual measures only if no automated measures exist.

G. DETAILED IMPLEMENTATION PLAN

This section contains a recommendation for the implementation of the Strategic actions by describing a timely arranged order of the actions.

G.1. PRIORITIZATION OF THE STRATEGIC ACTIONS

The above described recommended Strategic actions are very inhomogeneous in terms of financial and human resource needs and their overall effects. Therefore a prioritisation scheme was set up and recommended by the Consultants which may be considered by the Ministry whenever decisions are made on which Strategic action to initiate.

G.1.1. PRIORITISATION APPROACH

According to the used approach a combined effect and resource need estimations were assigned for each Strategic action. The combined effect is the combination of the following factors:

- Subjective priority of the Consultant relying on the priorities of the Justice sector's ICT managers and stakeholders,
 - Priority A – highest priority
 - Priority B – medium priority
 - Priority C – lowest priority
- Extent of the Strategic action which might be either of the following:
 - whole Justice Sector
 - one branch of the Justice Sector (e.g. prosecutorial branch, judicial branch, etc.)
 - one institution type (e.g. basic courts)
 - one institution
- Alignment with high level ICT goals
 - support of a few (1 or 2) of the high level ICT goals
 - support of some (3) high level ICT goals
 - support of several (4 or more) high level ICT goals

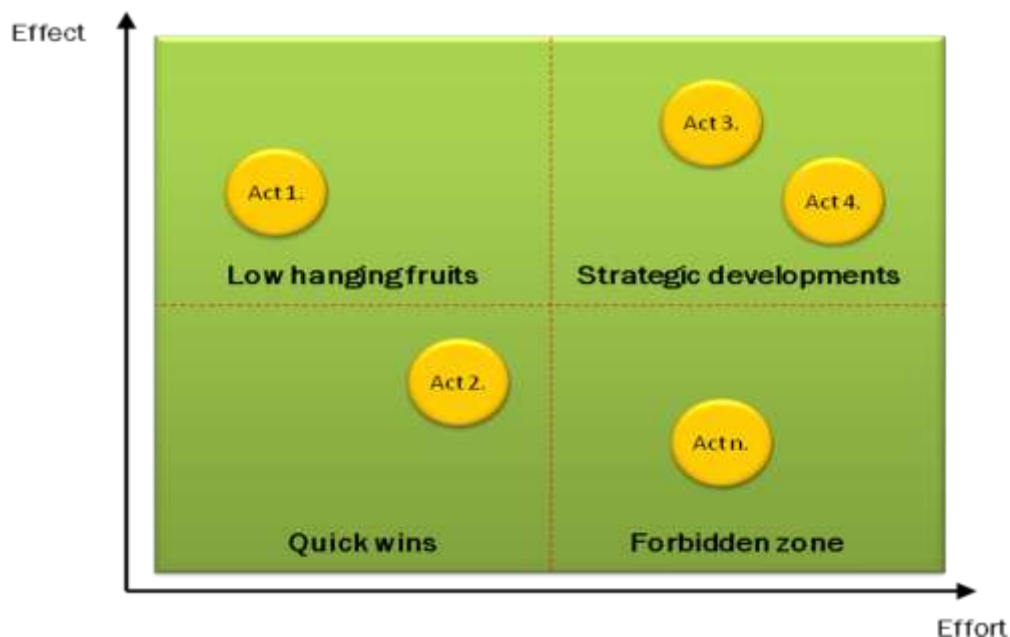
After transformation and combination of the above values, the **combined effect** of a Strategic action is a value of the scale 1-4.

Similarly the overall resource need is a combined value of the following factors:

- Financial resource needs
 - less than 50,000 EUR
 - between 50,000 EUR and 250,000 EUR
 - between 250,000 EUR and 1,000,000 EUR
 - more than 1,000,000 EUR
- Human resource needs (with not only actively participating staff members in action execution, but “passive” participants like trained employees as well)
 - less than 50 man days
 - between 50 and 250 man days
 - between 250 and 1000 man days
 - more than 1000 man days

The **combined effort** of a Strategic action is a value of the scale 1-4. Because financial and human resources are somewhat interchangeable, the combined effort is the maximum of the above financial and human resource need factors.

Next, the overall priorities may be formed as demonstrated on the following diagram:

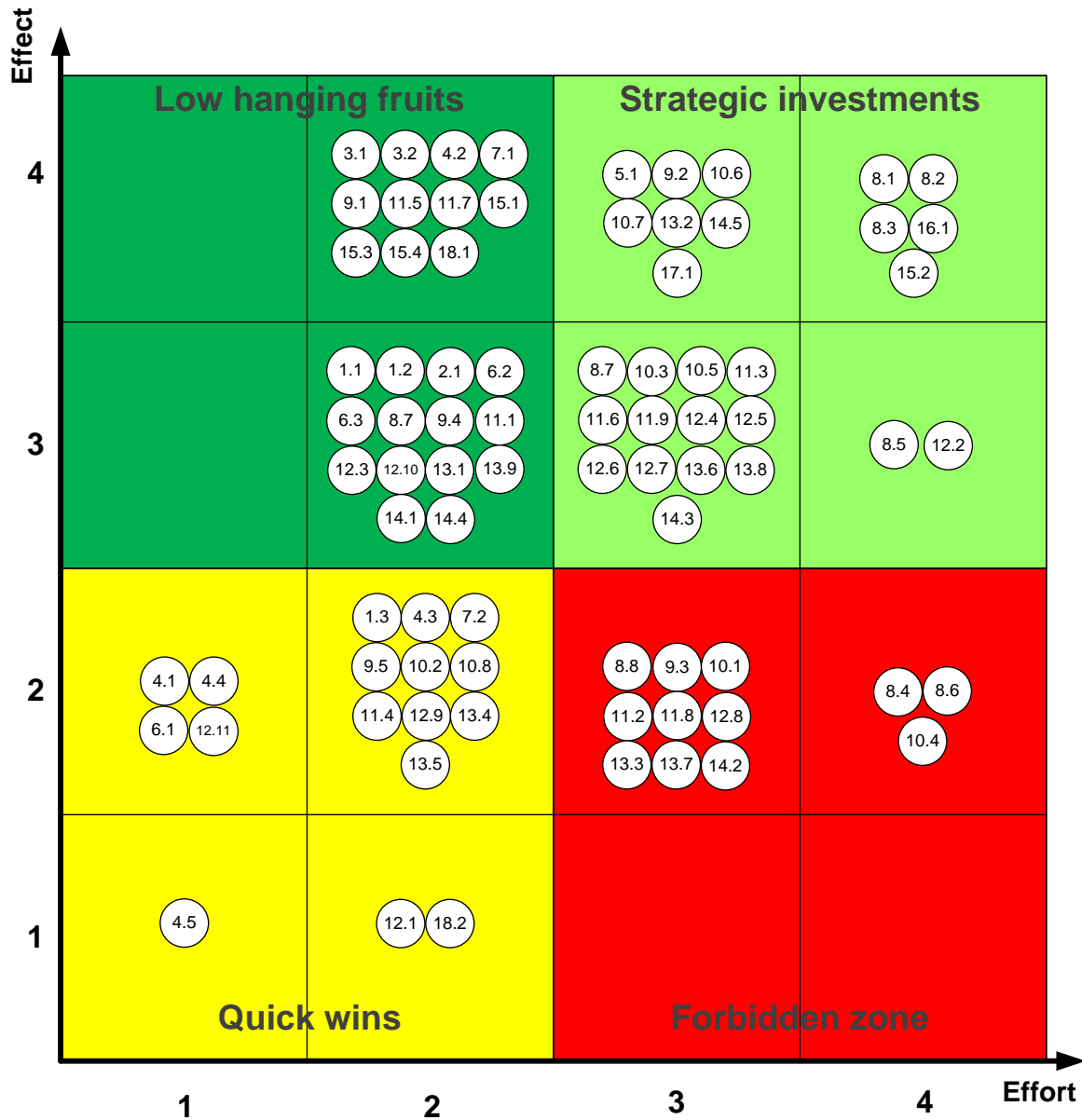


The four quadrants are the following:

- **Quick wins**
Strategic actions in this quadrant do not require high effort (investment), but their overall yield is not very high. These actions may be steps forward and usually worth the investments
- **Forbidden zone**
Strategic actions in this quadrant require high effort, and their yield is not very high. These actions should be avoided and executed only if some other high yield actions are dependent on them.
- **Low hanging fruits**
Strategic actions in this quadrant do not require high effort and their overall yield is high. These actions should be strongly preferred because of the good effect/effort ratio.
- **Strategic investments**
Strategic actions in this quadrant require high effort but their yield is also high. These actions should be individually and carefully investigated; preparing Feasibility Studies is a strongly recommended action before deciding on their execution. Another factor to consider is the availability of funds for them.

G.1.2. RECOMMENDED PRIORITISATION OF THE JUSTICE SECTOR STRATEGIC ACTIONS

Using the above described prioritisation approach; the Consultants' recommended combined priorities of the Strategic actions are the following:



The Strategic actions of the four categories are the following:

Forbidden Zone

ID	Strategic action
8.4	Extend functionally Case Management systems (i.e. full electronic case management)
8.6	Integration of Commercial Courts and functional improvement of their Case Management System
8.8	Implement a pilot Management Information System on Case Management systems to produce uniform analytical support
9.3	Upgrade for no-single-point of failure by implementing necessary redundancies for server components and networks
10.1	Define common master data used for all systems
10.4	Extend the document management capabilities of the implemented document management system
11.2	Establish a software license database

ID	Strategic action
11.8	Establish dedicated test environments for all IT systems filled with depersonalised data
12.8	Implement knowledge sharing functionality (mailing lists, Intranet pages, discussion forums) within the Justice Sector
13.3	Develop a proper authentication and authorisation scheme for accessing published documents on court portal
13.7	Implement personalisation and notification of registered users at centralised court portal
14.2	Define technical standards for the implementation of new ICT delivery channels

Quick wins

ID	Strategic action
1.3	Network with peer organisations in the EU and region and use experience from other countries that have already solved the organisation of the ICT sector in the judiciary
4.1	Define exact performance measures for each individual goal of the ICT Strategy
4.3	Define and implement technical level performance measures for internal services
4.4	Define and use an End User Satisfaction survey to assess user's perception on ICT services
4.5	Implement a unified and regular reporting service for management about the major ICT performance measures
6.1	Establish a yearly donor conference which demonstrates the results and the goals
7.2	Define profiles and implement Desktop virtualization solution
9.5	Achieve decentralisation and consolidation by using e-Government "cloud computing" infrastructure
10.2	Develop common look-and-feel standards for all web pages of the sector
10.8	Consolidate desktop printers and implement printing control
11.4	Develop capacities to analyse transactional logs
12.1	Implement a comprehensive Training Register to support the whole training process
12.9	Assess all locally developed applications and support the rollout of the most useful systems
12.11	Organise annual ICT conferences within the Justice Sector
13.4	Develop a common form management component to cover all forms to-be in electronic format
13.5	Enable electronic form submission for citizen's inquiries
18.2	Develop a dashboard for IT service level measurements

Low hanging fruits

ID	Strategic action
1.1	Adapt a service oriented approach in provision of IT services for end-users
1.2	Assembly of a service catalogue for all services provided by IT
2.1	Implement Awareness Campaign within the Justice sector on the importance of the ICT in modern justice processes
3.1	Prepare and implement long-term Feasibility Study and TCO methodologies for all ICT systems
3.2	Establish change management practices into implementation projects and regular two-directional information flow between ICT and end-users
4.2	Define Service Level Agreements with third party vendors and renew contracts
6-2	Establish ICT Strategy update responsibility within the Ministry
6-3	Define a uniform Business Case structure for ICT related investments
7.1	Develop technology standards for end-user environment
9.1	Develop and implement of Business Continuity plans and Disaster Recovery plans
9.4	Set up backup centre(s) and mechanisms for off-site storage for backup data
11.1	Declare IT security related roles and responsibilities by preparing an Information Security Policy and Security procedures
11.5	Review and strengthen authentication and authorisation methods
11.7	Raise the awareness of staff on IT security issues by development of an internal communiqué
12.3	Establish a scheme and written principles for ICT related trainings for the sector
12.10	Establish knowledge sharing functionality of the Service Desk
13.1	Setting up a common data structure framework for court information publication

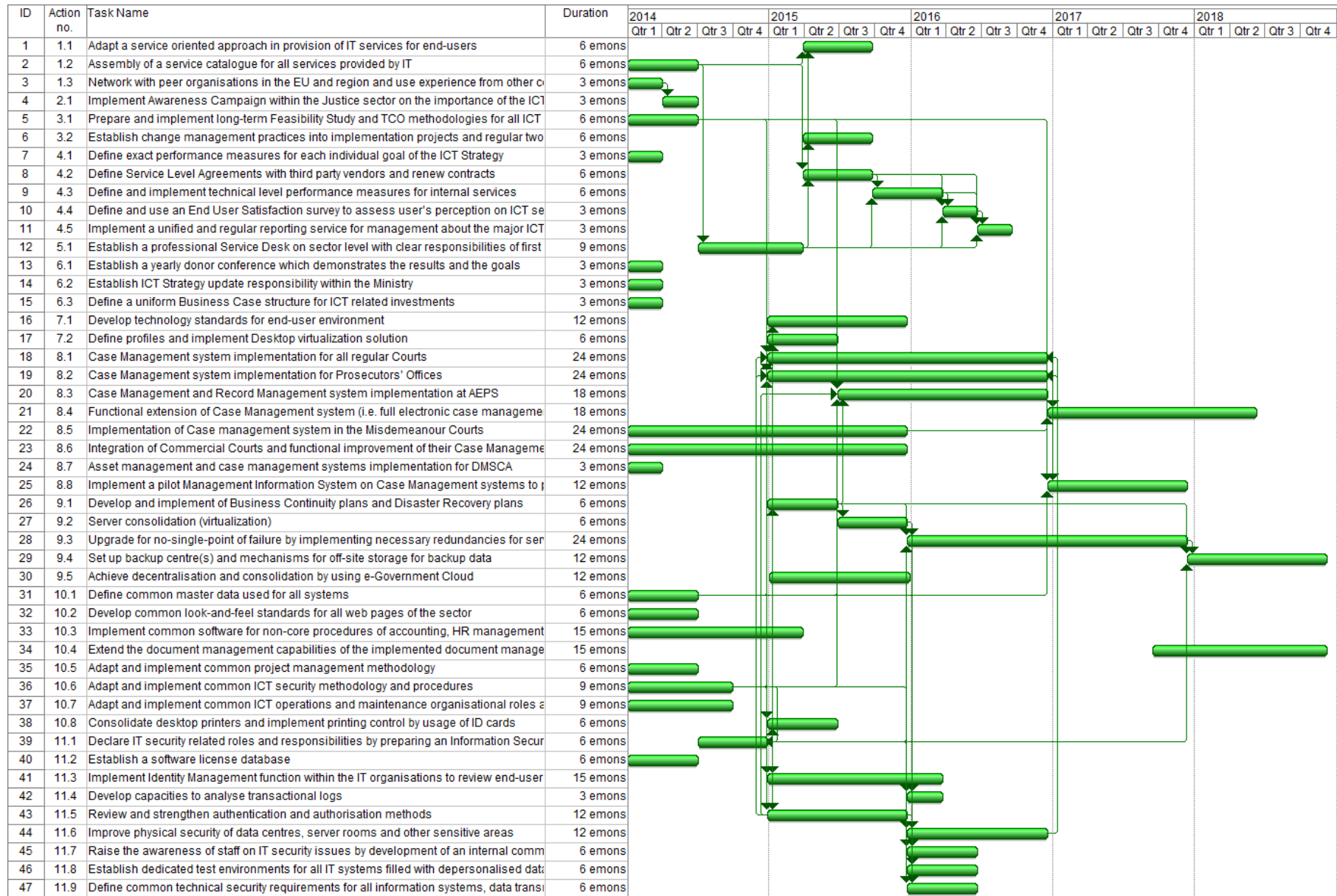
ID	Strategic action
13.9	Develop new portal for Judicial Academy which enables automatic publication of training calendar/ trainings courses / training materials
14.1	Consider all necessary legal changes required to implement proposed new ICT delivery channels in Justice Sector
14.4	Investigate most cost-effective approaches and technologies for the use in Justice Sector
15.1	Introduction of business process management in cooperation with the business areas
15.3	Establish sector-wide architecture management responsibilities to maintain a registry for ICT systems
15.4	Establish SOA on national e-Government infrastructure
18.1	Prepare feasibility studies for outsourcing of various activities

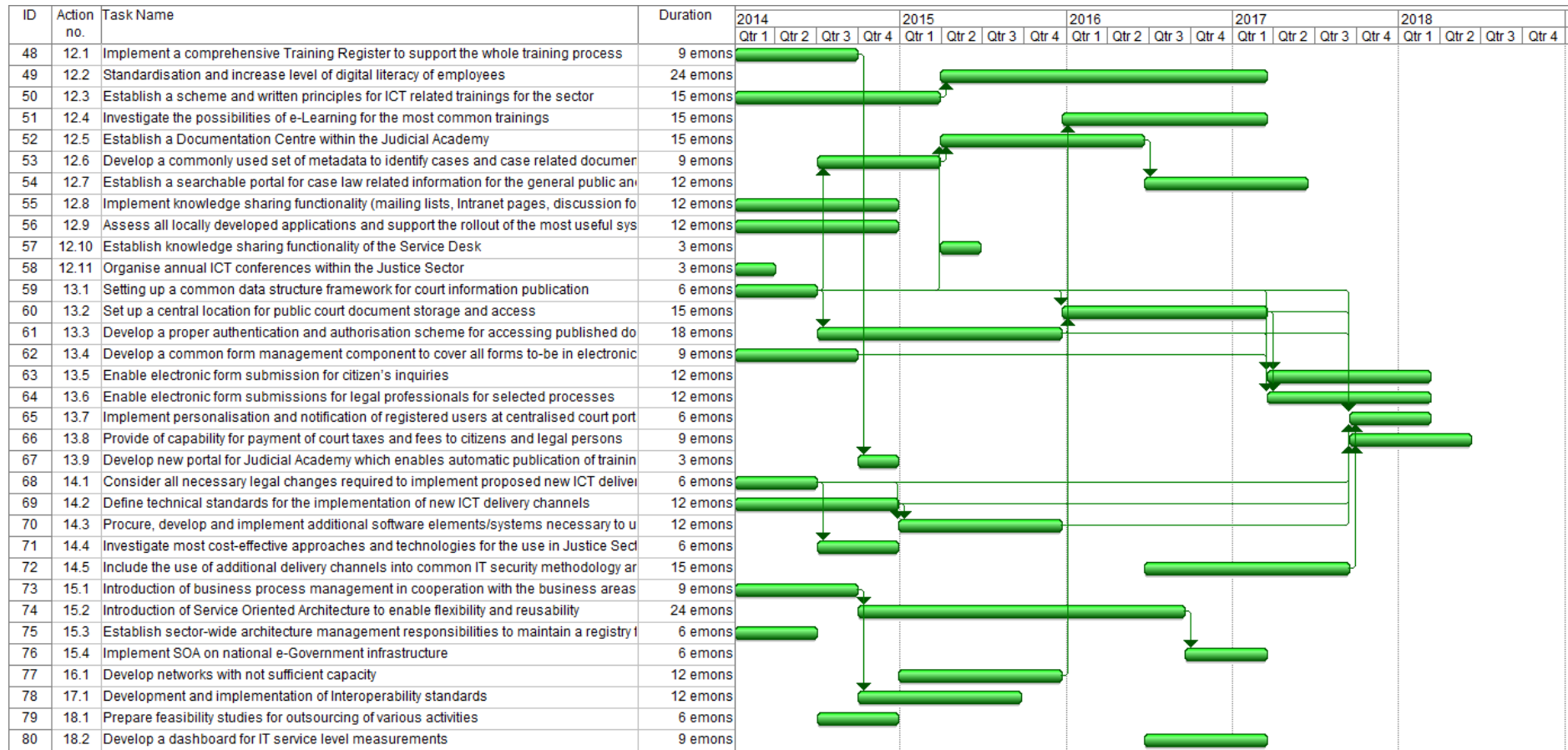
Strategic investments

ID	Strategic action
5.1	Establish a professional Service Desk on sector level with clear responsibilities of first line, second line and application support
8.1	Case Management system implementation for all regular Courts
8.2	Case Management system implementation for all Prosecutors' Offices
8.3	Implementation of Case Management and Records Management system at Prison Administration
8.5	Implementation of Case management system in the Misdemeanour Courts
8.7	Asset management and case management systems implementation for DMSCA
9.2	Server consolidation (virtualization)
10.3	Implement common software for non-core procedures of accounting, HR management, asset management
10.5	Adapt and implement common project management methodology
10.6	Adapt and implement common ICT security methodology and procedures
10.7	Adapt and implement common ICT operations and maintenance organisational roles and procedures
11.3	Implement Identity Management function within the IT organisations to review end-user access to software functions
11.6	Improve physical security of data centres, server rooms and other sensitive areas
11.9	Define common technical security requirements for all information systems, data transmission, authentication
12.2	Standardisation and increase of level of digital literacy of all employees
12.4	Investigate the possibilities of e-Learning for the most common trainings
12.5	Establish a Documentation Centre within the Judicial Academy
12.6	Develop a commonly used set of metadata to identify cases and case related documents
12.7	Establish a searchable portal for case law related information for the general public and external legal professionals
13.2	Set up a central location for public court document storage and access
13.6	Enable electronic form submissions for legal professionals for selected processes
13.8	Provide capability for payment of court taxes and fees to citizens and legal persons
14.3	Procure, develop and implement additional software elements/systems necessary to utilize the new ICT delivery channels
14.5	Include the use of additional delivery channels into common IT security methodology and procedures
15.2	Introduction of Service Oriented Architecture to enable flexibility and reusability
16.1	Develop networks with not sufficient capacity
17.1	Development and implementation of Interoperability standards

G.2. OVERALL SCHEDULE

Considering the above recommended priorities and the preconditions of the Strategic actions, a full overall possible project Implementation schedule of the Strategic actions is the following.





1.1 COST REVISION, COST VARIANTS AND RESOURCE UTILISATION SCHEDULE

Based on the above schedule, the cost-breakdown and resource utilisation breakdown may be calculated. In estimating the project costs the mean of the given cost range was used:

Cost range	Mean used for estimation
less than 20,000 EUR	10,000 EUR
between 20,000 and 100,000 EUR	60,000 EUR
between 100,000 and 500,000 EUR	300,000 EUR
more than 500,000 EUR	1,000,000 EUR

It was also supposed, that the project costs are distributed evenly during the whole implementation period of the given Strategic action, that is if it is 4 quarters long and its estimated mean cost is 300,000 EUR, then 75,000 EUR is allocated for each quarters affected by the action.

Although the donor organisations may provide significant funding for implementation projects, but the operational and maintenance costs should be paid from internal budget. This fact further limits the extent of Strategic action implementation, thus three cost variant were created (Low, Medium and High).

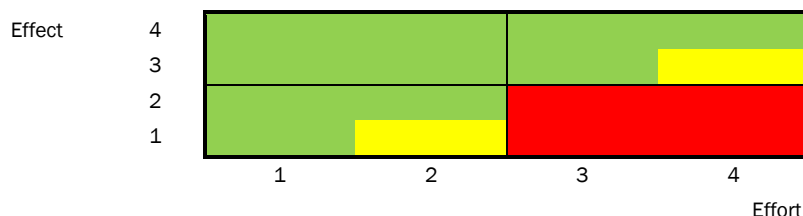
The one-by-one decision on the execution of the Strategic actions will depend on the actual budget status of the given years.

On the other hand some Strategic actions may generate revenues for the Justice sector (by additional fees for value added services) which should be considered at the moment of decision. In case of revenue generating Strategic actions, even initial implementation costs may be reduced by using a Public Private Partnership approach with the selected vendors.

In order to define the required Low Case, Medium Case and High Case of cost and human resource estimations, the following further considerations were made:

- Strategic actions were further classified into 3 categories:
 - “Forbidden fruit” actions as Low action priority projects
 - “Quick wins” and “Strategic investment” actions as Medium action priority IF their estimated effort on scale 1-4 is more than their estimated effect on the scale of 1-4.
 - All other actions as High action priority

This scheme is shown below:



Actions in the red, yellow and green zone correspond to the above categories.

Further possible fine tuning of cost and resource needs is to define alternative scope possibilities for the Strategic actions.

These scope reductions yield results only for large effort actions. After investigation, the following scope reduction possibilities were found:

ID	Strategic action	Scope reduction possibility	Reduced scope
8.4	Extend functionally Case Management systems (i.e. full electronic case management)	50%	Without implementing OCR capabilities
8.6	Integration of Commercial Courts and functional improvement of their Case Management System	75%	Only the most critical functional updates and integration features
9.3	Upgrade for no-single-point of failure by implementing necessary redundancies for server components and networks	30%	If only server redundancies are considered
9.4	Set up backup centre(s) and mechanisms for off-site storage for backup data	50%	If no separate backup centre is established, but any existing data centre may serve as a warm backup
10.3	Implement common software for non-core procedures of accounting, HR management, asset management	75%	Implement only a few basic functions
10.4	Extend the document management capabilities of the implemented document management system	25%	If the extension is confined only to the most frequently used document types
10.5	Adapt and implement common project management methodology	80%	In open source project management tool is selected
10.8	Consolidate desktop printers and implement printing control by usage of ID cards	80%	If the majority of the new centralised printers are leased or outsourced and not bought by the institutions.
12.2	Standardization and increase level of digital literacy of all employees	90%	If only the certifications of digital literacy are supported without mass trainings
12.4	Investigate the possibilities of e-Learning for the most common trainings	50%	If open source e-learning solution is implemented and training materials are developed in-house
12.3	Establish a searchable portal for case law related information for the general public and external legal professionals	50%	If only the most basic search criteria are implemented
13.3	Develop a proper authentication and authorisation scheme for accessing published documents on court portal	70%	In authentication and authorisation is implemented only for legal professionals and not for the general public
14.4	Procure, develop and implement additional software elements/systems necessary to utilize the new ICT delivery channels	50%	In the channels and services are restricted only to the most common ones
15.2	Introduction of Service Oriented Architecture to enable flexibility and reusability	50%	If the acquired application systems are already "SOA ready"
16.1	Develop networks with not sufficient capacity	75%	If governmental network can be used for WAN connections

Moreover in case of all tasks not involving software or hardware acquisition or development, the exclusive usage of internal resources is a significant cost reduction possibility. This means that no outside experience or consulting is purchased and staff members must learn to use the methodologies and tools.

Taking into consideration the above cost reduction possibilities and prioritisation, the implementation costs – as estimated by the Consultant – are expected as:

- Low cost variant 7,600,000 EUR
- Medium cost variant 11,620,000 EUR
- High cost variant 15,000,000 EUR

With these possible reductions the distribution of expected costs is demonstrated on the following diagram:

